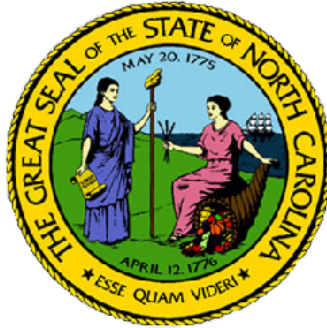


State of North Carolina



Summary Report

Assessment of Agency Compliance with Enterprise Security Standards

As Directed by Session Law 2003-153, Section 1(a), General Statute 147-33.82 (e1)
2003 Session of the North Carolina General Assembly

May 2004

Prepared by
Gartner, Inc.

Submitted to
State Chief Information Officer, George Bakolia

Table of Contents

1. STATEWIDE SECURITY ASSESSMENT EXECUTIVE SUMMARY	1
PURPOSE.....	1
APPROACH.....	1
OVERVIEW OF MAJOR FINDINGS.....	3
SECURITY ASSESSMENT PROJECT APPROACH AND METHODOLOGY.....	5
SECURITY REMEDIATION ESTIMATE OVERVIEW	10
2. SUMMARY OF MAJOR FINDINGS.....	13
STATEWIDE NOTABLE PRACTICES	13
OPPORTUNITIES FOR INFORMATION SECURITY POSTURE IMPROVEMENT.....	15
SUMMARY OF RECOMMENDATIONS.....	18
ENTERPRISE-LEVEL RECOMMENDATIONS	19
AGENCY-LEVEL RECOMMENDATIONS.....	24
3. DETAILED STATEWIDE SECURITY RECOMMENDATIONS	32
E1: ENHANCE THE ENTERPRISE-LEVEL SECURITY PROGRAM.....	32
E2: DEVELOP AND MAINTAIN STATEWIDE POLICY, STANDARDS AND PROCEDURES (PSPs).....	34
E3: IMPLEMENT FORMAL SECURITY TRAINING AND AWARENESS PROGRAM	34
E4: IMPROVEMENT RISK MANAGEMENT AND UPDATE BUSINESS CONTINUITY PLANS	35
4. DETAILED AGENCY-LEVEL SECURITY RECOMMENDATIONS	37
A1: INCREASE FUNDING TO AGENCIES FOR SECURITY	37
A2: DEVELOP AND MAINTAIN AGENCY POLICY, STANDARDS AND PROCEDURES (PSPs)	37
A3: INCREASE LEVEL OF SECURITY STAFFING.....	37
A4: IMPLEMENT FORMAL SECURITY TRAINING AND AWARENESS PROGRAM.....	38
A5: REPLACE OUTDATED DESKTOP OPERATING SYSTEMS.....	38
A6: IMPROVE AGENCY BORDER/PERIMETER DEFENSE.....	39
A7: IMPROVEMENT RISK MANAGEMENT AND UPDATE BUSINESS CONTINUITY PLANS.....	40
ADDITIONAL RECOMMENDATIONS FOR AGENCIES.....	41
5. DETAILED SECURITY FINDINGS BY ISO 17799 CATEGORY	44
1. SECURITY POLICIES, STANDARDS AND PROCEDURES (PSPs)	44
2. ORGANIZATIONAL SECURITY.....	45
3. ASSET CLASSIFICATION AND CONTROL.....	45
4. PERSONNEL SECURITY	46
5. PHYSICAL SECURITY	47
6. COMMUNICATIONS AND OPERATIONS MANAGEMENT	47
7A. ACCESS ADMINISTRATION.....	48
7B. ACCESS TECHNOLOGY	49
8. APPLICATIONS DEVELOPMENT AND MAINTENANCE	50
9. BUSINESS IMPACT/CONTINUITY MANAGEMENT	51
10. COMPLIANCE.....	52
6. STATEWIDE SECURITY EXPENDITURE SUMMARY	53

APPENDICES	60
APPENDIX A: AGENCIES AND COMMISSIONS INCLUDED IN THE ASSESSMENT AND ASSIGNED ASSESSMENT VENDOR	61
APPENDIX B: ISO 17799 — SYNOPSIS	63
APPENDIX C: SUPPORTING GRAPHICS	66
APPENDIX D: SECURITY POLICY GAP ANALYSIS SUMMARY	70
APPENDIX E: AGENCY SECURITY POSTURE	73
APPENDIX F: SECURITY REMEDIATION ESTIMATE DETAIL	74
APPENDIX G: DISTRIBUTION OF AGENCY SECURITY SCORES	83

Table of Figures

Figure 1: Planned Security Practices (e.g., Quality)	5
Figure 2: Actual Security Practices (e.g., Execution)	6
Figure 3: Agency Security Assessment Posture	7
Figure 4: Agency Security Posture by Size	8
Figure 5: Agency Security Posture by Assessment Group	8
Figure 6: IT Security Expenditure as a Percentage of Operating Budget	53
Figure 7: Physical Security Expenditure as a Percentage of Operating Budgets	54
Figure 8: Business Continuity Planning Expenditure as a Percentage of Operating Budgets	55
Figure 9: Security and BCP Expenditures as a Percentage of Total Budget	56
Figure 10: FY03–04 Security and Business Continuity Expenditure Detail	58
Figure 11: Average Security Quality and Execution Score by Sub-Category	67
Figure 12: Average Security Quality and Execution Score by Sub-category	67
Figure 13: Average Security Quality Score vs. Average Security Execution Score (by Category)	68
Figure 14: Average Security Scores by Agency Size	69
Figure 15: Average Security Scores by Project Grouping	69
Figure 16: Sizes of Agencies by Group	69
Figure 17: Translation of Security Assessment Scores	73
Figure 18: Cost Estimates by Security Finding — Expense/Capital Breakout	74
Figure 19: Cost Estimates by Security Finding — Expense/Capital Summary	75
Figure 20: Workday Estimates for Enterprise-Level Security Recommendations	76
Figure 21: Cost Estimates for Enterprise-Level Security Recommendations	77
Figure 22: Ongoing Operating Cost Assumptions for Enterprise-Level Security Recommendation	78
Figure 23: Workday Estimates for Agency-Level Security Recommendations	79
Figure 24: Cost Estimates for Agency-Level Security Recommendations	80
Figure 25: Ongoing Operating Cost Assumptions for Agency-Level Security Recommendations	81

1. Statewide Security Assessment Executive Summary

Purpose

In response to provisions of G.S. 147-33.82 (e1) of North Carolina Session Law 2003-153, which requires the State Chief Information Officer (CIO) to conduct an assessment of the information security posture of all Executive Branch agencies, the State of North Carolina initiated a statewide security assessment in September of 2003. The assessment process was designed to provide State decision-makers with:

The State Chief Information Officer shall assess the ability of each agency to comply with the current security enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the standards in each agency and an assessment of each agency's security organization, network security architecture, and current expenditures for information technology security. The assessment shall also estimate the cost to implement the security measures needed for agencies to fully comply with the standards. Each agency subject to the standards shall submit information required by the State Chief Information Officer for purposes of this assessment.

Section 1 (a) G.S. 147-33.82(e1) of North Carolina Session Law 2003-153

- A global view of the security posture of those agencies;
- An understanding of current expenditures for information security as reported by agencies; and
- Specific assessment findings in detail sufficient to permit the State to prioritize and budget for required security enhancement efforts

Approach

The assessment effort was conducted by a group of eight security vendors selected and retained by the State Office of Information Technology Services (ITS). A Security Project Management Office (PMO) was set up by the State to manage the assessment project. The State engaged Gartner, Inc. to manage the PMO, normalize¹ the data, and produce a draft of the Statewide Assessment for the CIO's review. Security vendors were assigned to agencies by Information Technology Services (ITS), ensuring that vendors were not assigned to agencies where they had performed significant security projects in the past. The goal of the assignments was to provide an independent and unbiased assessment. The vendors used assessment tools and templates developed by the State Information Security Office's PMO to ensure uniformity of process and consistency of results.

¹ Normalization of data involved reviewing the results of the vendor assessments, and ensuring that similar observations were scored in the same way, across agencies. This process was intended to make certain that no individual assessment vendor would unintentionally skew the results because the vendor graded more harshly or leniently than another. The PMO worked with each vendor on each assessment to mutually agree on any changes that resulted from normalization, but ultimate scoring was the vendors' decision.

These tools and templates incorporated the statewide blended security framework including Federal and State legislative requirements and the ISO 17799² information security standard. The State Chief Information Security Officer directed project operations through the PMO.

The statewide assessment effort divided the agencies into three groups to manage the large number of agencies. The agency assessments were conducted between September 2003 and March 2004. Analysis and findings were developed in April 2004. Findings in this statewide report are a reflection of the agency security posture on the date that the vendor completed the assessment. Adjustments to the individual agency scores have been incorporated into the reports if an agency has submitted a correction to the findings. The PMO did not adjust scores if an agency indicated that it has made improvements or taken actions subsequent to the vendor's assessment.

The ISO 17799 framework includes a series of categories to structure a security program. The *Access* category of the standard includes the operations and technologies associated with directly defending against unauthorized access to the State's network. In order to emphasize the importance of this portion of the assessment, the PMO divided the category into two sub-categories: *7a. Access Administration*; and *7b. Access Technology*. (See Section 5, pages 47 and 48 for more information.)

Recommendations for remediation at both the Enterprise level and the Agency level, including costs (initial and ongoing), have been developed and are included in detail in this report.

The following sections provide a summary-level analysis of the major findings of the assessment. Detailed findings, including notable practices and opportunities for improvement by category, are provided further into the report.

² ISO 17799 is an internationally recognized information security standard adopted by the International Standards Organization.

Overview of Major Findings

Notable Practices

There are some excellent building blocks currently in place for the State's security efforts going forward. Many of the State agencies have some outstanding aspects within their current security programs that can be used to build the overall quality and performance of the agencies' security program. Key notable practices that were found across many of the existing security programs are bulleted below. Additional notable practices are included in the detailed findings.

At most agencies:

- Security importance is recognized
- The statewide security framework is in place
- Virus prevention is practiced
- Keys and access cards are managed
- Undesirable user accounts are disabled
- Unauthorized modems are removed

Opportunities for Improvement

This assessment identified key opportunities for improving the statewide security posture. These areas address opportunities that should be pursued at the statewide level, consistently throughout the State. The PMO has provided the agencies with individual assessment reports that address unique, tailored, agency-specific improvement opportunities. Key opportunities for improvement identified in the assessment are bulleted below. Additional opportunities for improvement are included in the detailed findings.

At most agencies:

- Funding for security is insufficient
- Security policies, standards and procedures are deficient or absent
- Levels of staffing for security are insufficient
- Security experience and training is lacking
- Desktop operating systems are outdated
- There are gaps in agency border/perimeter defenses
- Risk and business continuity management are outdated and/or incomplete

Summary of Recommendations

The assessment recommendations have been broken out into Enterprise-level recommendations and Agency-level recommendations. Enterprise recommendations (noted by E#) are remediation activities that should be performed at the statewide level to allow the State to gain economies of scale and to ensure consistency across agencies. Agency recommendations (noted by A#) are remediation activities that are specific to agencies.

Although the State's security posture is not as strong as it could be, the State has recognized the importance of security and has positioned itself to strengthen its information security program. To do so, the State should consider the following recommendations:

Enterprise Recommendations are:

- E1: Increase funding to enhance the enterprise security program
- E2: Complete statewide security policies, standards and procedures
- E3: Improve security awareness and training
- E4: Improve risk management and update business continuity plans

Agency Recommendations are:

- A1: Increase funding to agencies
- A2: Improve agency security policies, standards and procedures
- A3: Increase level of security staffing
- A4: Improve security awareness and training
- A5: Replace outdated desktop operating systems
- A6: Improve agency border/perimeter defenses
- A7: Improve risk management and update business continuity plans

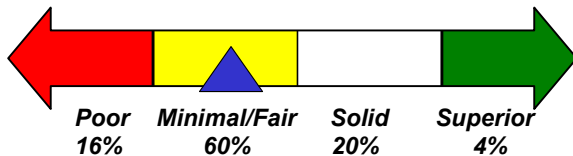
Security Assessment Project Approach and Methodology

The assessment methodology scored agencies against two scoring categories: “Quality” and “Execution”. The purpose of these two dimensions is to capture the agencies’ level of security planning, as well as the agencies’ actual securing of the information assets. Scoring was administered on a graduated scale, where a score of “1” represents the highest or best possible mark, and a score of “4” represents the lowest or worst possible mark.

Quality Score Dimension

Figure 1 depicts the average quality score (triangle) from the assessments. In general, State agencies possess Policies, Standards and Procedures (PSPs) that are considered “Minimal/Fair”, given the State’s information protection requirements. This means that there are severe deficiencies and gaps in the agencies’ posture and that there is much work to be done to properly protect the State. Below each score is the percentage of agencies that achieved that rating.

Figure 1: Planned Security Practices (e.g., Quality)



The Quality score represents whether an agency has effectively and completely addressed its information security requirements through its Policies, Standards and Procedures (PSPs).

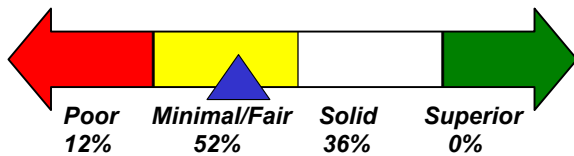
Quality scores mean the following:

- “Superior” indicates that the PSPs conform to best practices
- “Solid” indicates that PSPs meet requirements
- “Minimal/Fair” indicates that the PSPs are deficient
- “Poor” indicates that the PSPs do not meet requirements

Execution Score Dimension

Figure 2 depicts the average score (triangle) from the assessments. In general, State agencies have deployed security measures that are considered “Minimal/Fair”, given the State’s information protection requirements. Significant room for improvement exists. This means that there are severe deficiencies and gaps in the Agency posture and that much work needs to be done to properly protect the State’s information assets. Below each score is the percentage of agencies that achieved that rating.

Figure 2: Actual Security Practices (e.g., Execution)



The Execution score represents whether an agency has deployed information security Policies, Standards and Procedures in an encompassing fashion. Execution scores mean the following:

- “Superior” indicates that the PSPs are fully or universally deployed
- “Solid” indicates that the PSPs are deployed for critical areas only
- “Minimal/Fair” indicates that there are significant gaps in the deployment of PSPs
- “Poor” indicates that there are no PSPs in effect or implemented, or that PSPs are still in development

Agency Security Posture Results

Figure 3 plots the Quality and Execution scores of all agencies onto a “quadrant” diagram. Agencies that have stronger security programs chart onto the upper-right quadrant, whereas agencies that have weak security postures chart onto the lower-left quadrant. **Any program not in the upper-right quadrant is deficient in some manner.** A point representing the statewide average has been added to the chart and is circled in red.

To clarify the State’s security posture, the PMO has established a grading system that enables the State to simplify the interpretation of the scores. Using this scale, the State’s security posture is **Minimal/Fair**. This means that there are severe deficiencies and gaps and that much work needs to be done to properly protect the State’s information assets.

Figure 3: Agency Security Assessment Posture

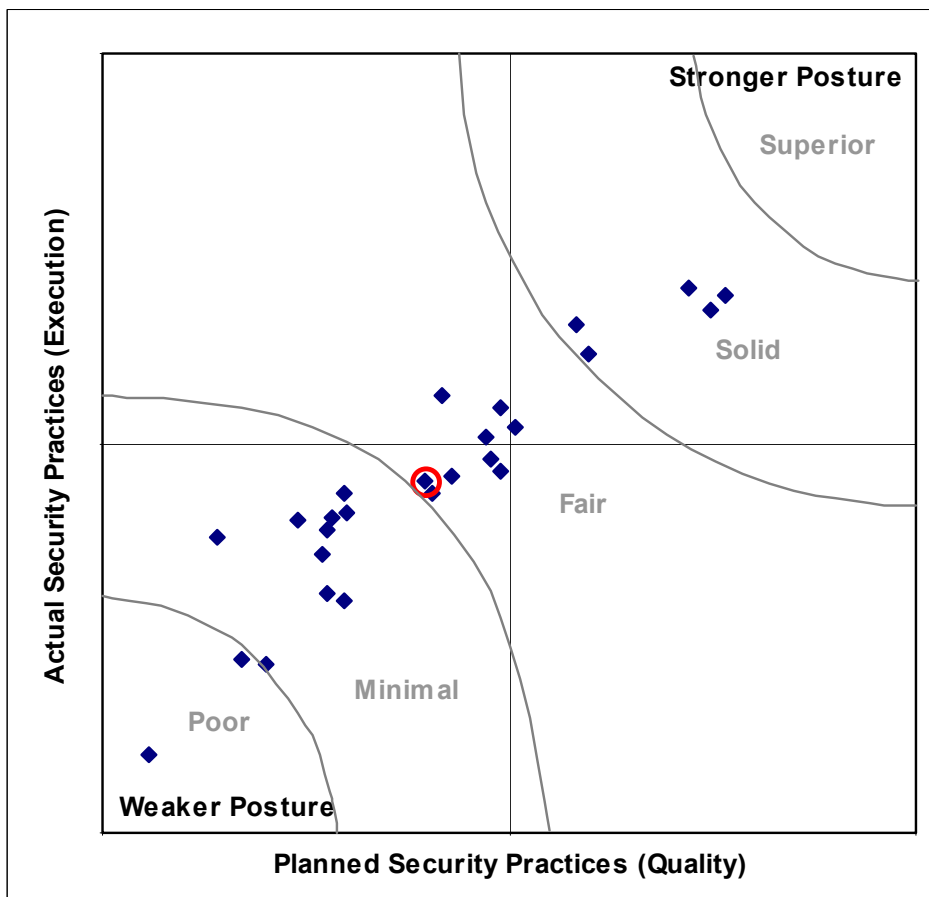


Figure 3 also highlights that many State agencies have weak security postures. With only 23 percent of assessed agencies falling within the upper-right quadrant, information security within agencies across the State needs to be improved to effectively address the State's security requirements.

It might not be necessary that all agencies be brought to a "best-practice" security posture. Such an effort would be inappropriately expensive. In some areas, a "Solid" performance in security is sufficient. The State should require that each agency conduct a risk assessment annually, to establish what the current risks are and what the additional remediation strategies should be.

Figure 3 also shows that several agencies have execution scores that are higher than their quality scores. This indicates that an agency's information security staff has devoted its time to actually supporting security efforts, and not necessarily to documenting them. Lack of documentation is an indicator of severe resource constraints that hinder the staff's ability to formalize policies, standards and procedures. The lack of documented PSPs puts the State at risk of losing critical institutional knowledge when employees leave or transfer to new positions.

Figures 4 and Figure 5 show the average scores of the agencies by size of agency and by assessment group.

Figure 4: Agency Security Posture by Size

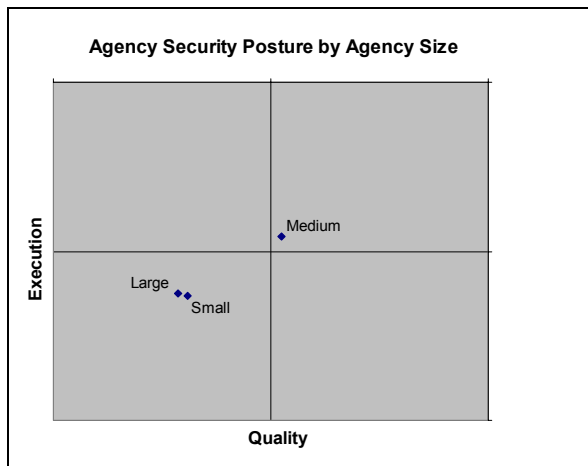
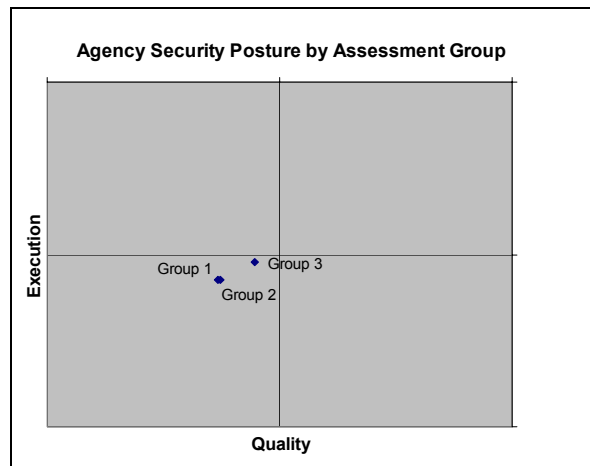


Figure 5: Agency Security Posture by Assessment Group



Several observations regarding the assessment should be noted:

- It was not practical to conduct all of the assessments simultaneously; therefore, the agencies were organized into three groups. Agencies that were in the second and third groups had more time to prepare for the assessment than the agencies in the first group did.
- The average scores of the Group 3 agencies were slightly better than the averages of Groups 1 and 2; however, Group 3 included the largest concentration of agencies with legal mandates to secure their data.
- The medium-size agencies have, on average, a better score than the other agencies. This may be because the medium-size agencies have a higher percentage of legally mandated security requirements.
- The small agencies and the large agencies have virtually the same average scores.
- Many agencies began to make improvements right after the vendors completed the data-gathering portion of the assessment.
- A majority of the agencies were performing security tasks despite a lack of documented procedures.
- The averages for Groups 1 and 2 were virtually the same.

Security Remediation Estimate Overview

The first question that needs to be answered when estimating the cost to close the existing gaps is: "How far should the State go?" Gartner estimates that it takes an average of 18 months (excluding the time to plan the project and get funding) to move from one level of maturity to the next. Since the State is already at risk given its current security posture ("Minimal/Fair"), this estimate means the State needs to act promptly to implement a more encompassing security program. The longer it takes to implement a program, the greater the hurdles the State will have to leap to meet a rapidly changing security environment. Gartner recommends that the State move its security posture up at least one maturity level to a ranking of "Solid".

"The average organization spent 7% of revenue on IT in 2003. Gartner estimates that the average organization spent 5.4% of its IT budget on security in that same period. Thus, security spending will consume an average of 0.38% of revenue, annually. Disaster recovery spending was an incremental 3–4% during the same period (or 0.2% of revenue)."

Source: Gartner, Inc.

The State spends about \$14,016,000 on security-related hardware, software and services. This represents about 0.15 percent of the total operating budget. Based on Gartner's research, this means that the State has been spending only 50 percent of what Gartner would expect an enterprise to spend on developing and maintaining an effective security program that would ensure protection of confidential data and information resources.

Gartner recommends that the State spend the estimated \$53 million³ identified in this report to bring the agencies up to a stable and reasonably secure posture. To ensure security on an ongoing basis, the State should allocate 0.38 percent of its total operating budget to support and to maintain the technologies and programs set in place.

Gartner further recommends that the State conduct a formal security reassessment on a three- to five-year cycle. Throughout the remediation period, the State should carefully and continuously monitor the progress made in remediation and security posture.

At the end of the remediation period, a formal reassessment should be conducted to evaluate how much improvement was achieved, and to identify any new enterprise-level or agency-specific threats that may have arisen.

³ Of the approximately \$53 million identified need, \$39 million represents replacing outdated desktops that severely hinder the State's ability to protect its information assets.

Gartner believes that this level of investment in security is necessary not only because of legal mandates, but also because of the nature of the information entrusted to the State by its constituents.

In addition to direct security expenditures, the State should increase its Business Continuity Planning expenditures. The State currently spends \$5,128,100 on Business Continuity Planning, which represents approximately 0.06 percent of the total agency operating budgets. Gartner research indicates that a state the size of North Carolina should spend approximately 0.20 percent of revenue. For North Carolina, this would be \$18,208,000 — a difference of \$13,079,900 from current spending levels.

Statewide Security Assessment Summary Report

Version No. FV01

May 2004

Table 1: Budget Estimates by Recommendation

Finding	Recommendation	Enterprise		Agency		Total	
		Total Initial Outlay	Ongoing Operating Costs	Total Initial Outlay	Ongoing Operating Costs	Total Initial Outlay	Total Ongoing Operating Costs
Insufficient Funding	E1: Increase Funding to Enhance Enterprise Program Office	2,026,400	1,821,360			2,026,400	1,821,360
	A1: Increase Funding to Agencies				(1) 15,196,640		15,196,640
	Subtotal					2,026,400	17,018,000
Deficient and Absent Policies, Standards, and Procedures	E2: Complete Statewide Security Framework	387,200	35,000			387,200	35,000
	A2: Improve Agency Security Policies, Standards, and Procedures			1,542,800	364,000	1,542,800	364,000
	Subtotal					1,930,000	399,000
Insufficient Levels of Staffing	A3: Increase Level of Security Staffing			2,144,800	2,144,800	2,144,800	2,144,800
Security Experience is Lacking	E3: Improve Enterprise Security Awareness and Training	504,000	205,600			504,000	205,600
	A4: Improve Agency Security Awareness and Training			431,200	436,800	431,200	436,800
	Subtotal					935,200	642,400
Outdated Desktop Operating Systems	A5: Replace Outdated Desktop Operating Systems			(3) 38,820,000		38,820,000	
Gaps in Agency Border / Perimeter Defense	A6: Improve Agency Border / Perimeter Defense			1,544,880	374,800	1,544,880	374,800
Outdated and Incomplete Risk and Business Continuity Management	E4: Improve Risk Management and Business Continuity Plans	2,032,800	1,307,990			2,032,800	1,307,990
	A7: Improve Risk Management and Business Continuity Plans			3,466,800	(2) 11,771,910	3,466,800	11,771,910
	Subtotal					5,499,600	13,079,900
Totals:		4,950,400	3,369,950	47,950,480	30,288,950	52,900,880	33,658,900

Notes:

(1) The estimate for recommendation A1: *Increase funding to Agencies* represents the difference between what Gartner recommends the State spend on security (\$20,579,000) and the sum of all other recommendations. These funds would be allocated to the agencies based on their security posture.

(2) The estimate for recommendation A7: *Improve Risk Management and Update Business Continuity Plans* represents the difference between what Gartner recommends the State spend on Business Continuity Planning (\$18,208,000) and the amounts allocated for Business Impact Analyses and Risk Planning. These funds would be allocated to the agencies based on their Business Continuity Planning posture.

(3) Initial outlays for desktop upgrades are necessary to enable the agencies to deploy secure desktop operating systems. The ongoing maintenance of the machines should be included in the normal operating budgets of the agencies.

2. Summary of Major Findings

This section provides an overview of major assessment findings and related analysis. Additional supporting detail follows in subsequent sections and in the Appendices.

Statewide Notable Practices

During the course of the agency-level assessments, several notable practices were found. The assessment deemed items *notable* if the practices reflect generally accepted industry security standards and meet State and agency requirements. Notable practices mean that agencies responded at a level of 60 percent or greater. These practices represent a strong foundation toward continuously improving the State's security profile.

Some notable practices in place at more than 60 percent of the agencies include the following:

Security Importance:

~100% of agencies scoring Superior

While formal programs that include performance metrics may not be in place at many agencies, the importance of security is recognized by the agencies, as evidenced by the fact that the agencies were dedicated, diligent, and remained on schedule throughout the assessment process. All agencies assessed have designated security agency liaisons. Additionally, many agency executives attended the debriefings. While limitations in funding and staffing inhibit agency ability to implement security programs, agency leaders recognize the importance of information security.

Removal of Unauthorized Modems:

88% of agencies scoring Solid to Superior

Modems attached to computing equipment that is attached to the network can provide a bridge between secured and unsecured networks. The agencies do an effective job of removing these modems to ensure that an individual user does not inadvertently open an entry point to the secure networks.

Undesirable User Accounts:

85% of agencies scoring Solid to Superior

The agencies effectively manage unsecured and temporary user accounts (e.g., guest accounts). Since most new computing equipment is shipped with open access to these accounts, their removal is critical to ensuring that the simplest way to "hack" into a network is closed.

Virus Prevention:

84% of agencies scoring Solid to Superior

The State does an effective job preventing viruses from causing extensive damage to the State's network. This is verified by the relatively low rate of virus outbreak at the State agencies.

Almost all agencies use some form of centralized virus control. While the task of maintaining up-to-date virus files is very labor-intensive, these activities are achieving the desired outcome.

Keys and Access Cards:

81% of agencies scoring Solid to Superior

The agencies are diligent about controlling physical keys and access cards to buildings. With a small number of exceptions, access cards were properly displayed and, in many cases, individuals were challenged while on agency premises. This layer of physical security assists in ensuring that physical assets at the State are protected and that no unauthorized persons gain access to State facilities.

Security Framework:

62% of agencies scoring Solid to Superior

The State has developed a standard framework for security based on ISO 17799. This framework provides a good foundation for the agencies to develop their tailored PSPs. Many agencies that do not have their own PSPs default to the State's framework.

Opportunities for Information Security Posture Improvement

This assessment identified key opportunities for improving the statewide security posture. These areas address opportunities that should be pursued consistently throughout the State. In the individual agency reports, the assessment addresses unique or agency-specific improvement opportunities. The opportunities outlined below are included because they demonstrate at least one of following characteristics:

- The opportunity impacts a large number of agencies
- The opportunity represents a potentially severe compromise of the entire State's security posture
- In some cases, centralized efforts would provide significant economies and efficiencies of scale

Overall Insufficient Funding For Security:

~100% of agencies scoring Poor

While agencies demonstrated a sincere desire to properly protect State information, most agencies indicated a lack of funding as the largest inhibiting factor. A lack of funding often stems from a number of factors, including the distributed nature of State budgeting, tight budgets, and natural resistance to funding "overhead" vs. programmatic expenditures.

Insufficient Levels of Staffing:

84% of agencies scoring Minimal/Fair to Poor

Most agencies lack sufficient staff to provide adequate security. In many cases, there is either no staff dedicated to security (security responsibilities are shared, with no person held accountable), or too few staff with assigned security responsibilities. This resource issue affects an agency's ability to address emergent issues, to identify gaps or intrusions, and to defend against threats.

Security Experience and Training is Lacking:

76% of agencies scoring Minimal/Fair to Poor

Agency security experts and end users receive insufficient security training. This situation exposes an agency to unintentional security risks due to ignorance or misunderstanding. Additionally, IT staff members performing security roles are not fully equipped to address an agency's specific security requirements. Most agencies do not have a program in place to ensure that their staff remains current on the latest security issues and resolutions.

Outdated Desktop Operating Systems:

72% of agencies scoring Minimal/Fair to Poor

Many agencies are running desktops with obsolete operating systems (DOS, Windows 3.1 and Windows 9x). These operating systems do not provide effective password or other information security protections. Insecure desktops expose the State network to easy intrusion. Without

secure desktops, confidential data is exposed and agency systems can be used to intrude on other State systems.

Outdated and Incomplete Risk and Business Continuity Management:***69% of agencies scoring Minimal/Fair to Poor***

Most agencies lack basic business continuity processes and tools, including identification of key risk, recovery plans, recovery sites, staffing, etc. Additionally, 77% of the agencies have not conducted a Business Impact Analysis in the recent past. In fact, many agencies turned in their original Year-2000 business continuity plan as their most recent planning effort. Most agencies, in the event of a disaster (fire, flood, electrical outage, etc.), have no realistic means to quickly recover their technology. This lack of disaster recovery preparedness exposes citizens to the loss of services in case of a disaster. As the State increases its dependence on technology and extends its services to its constituents via technology, this issue will only increase.

Gaps in Agency Border/Perimeter Defense:***64% of agencies scoring Minimal/Fair to Poor***

The ITS organization within North Carolina operates the State network as an Internet Service Provider (ISP); however, all individual agencies are expected to control their own virtual boundaries/perimeters, based on their specific needs. An agency that is responsible for a significant amount of confidential data would be expected to have greater border/perimeter protection than an agency that is responsible for primarily public data. Included below are three of the most common ways for an agency to protect its network from unauthorized parties.

Firewalls

A firewall is used to ensure that the agency is protected from unauthorized access to data. A firewall acts as a filter to permit or deny access to the agency information, based on predefined permissions. These agency borders/perimeters are compromised by a lack of effective firewall technologies, improperly configured firewalls or outdated technology. Even secure areas of the State's network are exposed to intrusion due to interconnectivity between secure agency networks and insecure ones.

Modems

There are still three agencies that have desktops with modems attached. These agencies should immediately disable unauthorized modems in computers that are able to connect to the State network, because it creates an unauthorized access tunnel to State systems.

Wireless

Lastly, 84% of the agencies have no repeatable processes in place to test for unapproved wireless networks. The lack of testing means that there is no way to validate that a wireless device has not opened a doorway to the agency's network.

Deficient and Absent Security Policies, Standards and Procedures (PSPs):

60% of agencies scoring Minimal/Fair to Poor

Most agencies do not have adequate internal PSPs. In some cases, the agencies are missing a definition/description of key security requirements, and/or have gaps in policies. Additionally, 73 percent of agencies do not have adequate processes in place to update the PSPs, to ensure that they remain current and are applicable for ensuring that employees can protect the State's assets.

Summary of Recommendations

The assessment recommendations have been broken out into Enterprise-level recommendations and Agency-level recommendations. Enterprise recommendations (noted by E#) are remediation activities that should be performed at the statewide level to allow the State to gain economies of scale and to ensure consistency across agencies. Agency recommendations (noted by A#) are agency-specific remediation activities that are specific to agencies.

As the data were analyzed, it became apparent that there were some opportunities for improvement at the Enterprise level and some opportunities for improvement at the Agency level.

Enterprise Recommendations are:

- E1: Increase funding to enhance the enterprise security program
- E2: Complete statewide security policies, standards and procedures
- E3: Improve security awareness and training
- E4: Improve risk management and update business continuity plans

Agency Recommendations are:

- A1: Increase funding to agencies
- A2: Improve agency security policies, standards and procedures
- A3: Increase level of security staffing
- A4: Improve security awareness and training
- A5: Replace outdated desktop operating systems
- A6: Improve agency border/perimeter defense
- A7: Improve risk management and update business continuity plans

The following recommendations were developed by analyzing the agency assessments, and determining what steps to take to best propel the State forward in its security posture. Remediation recommendations describe the required steps, time and staffing requirements, one-time cost to implement the activities, and recurring costs to maintain the remediation.

All staffing costs are estimated at a contractor rate of \$150 per hour, or \$70 per hour for internal resources⁴. One full-time equivalent (FTE) is defined as 220 workdays.

⁴ The rate of \$150 per hour for external consultants was an average of the rates of the vendors in the security assessment. The rate of \$70 per hour for internal resources is a blend of the rate for an internal resource (\$60 per hour) and the hourly rate of the ITS personnel provided to the agencies.

Enterprise-Level Recommendations

E-1: Increase Funding to Enhance the Enterprise-Level Security Program

Findings Summary	Insufficient funding for Enterprise Security Initiative — The State does not provide sufficient funding to implement the infrastructure required to secure the State's assets.
Corrective Action	By augmenting the <i>Enterprise Level Security Program</i> , all agencies would benefit from these specific funds earmarked for security. Additionally, the State's Information Security Office needs a general security fund for use in leveraged security initiatives (ones that span multiple agencies) as well as compliance audits and funding of penetration tests. The Enterprise Security Program Office should be responsible for ensuring that the additional funding that is being made available to the agencies is being used for security and not for general administrative or programmatic purposes.
Benefit	By augmenting the existing Enterprise program, the State will leverage economies of scale and provide tailored services. Specifically earmarking security spending will allow its success to be tracked more effectively. This funding will also support the consistent prioritization and implementation of security measures, rather than the present spotty and <i>ad hoc</i> process.
Estimated Cost	<p>Total one-time costs to effect the improvements to the program: \$2,026,000</p> <p>Annual funding to maintain improvements: \$1,821,000</p> <p>This funding is exclusive of the amounts necessary to implement the remaining recommendations in this report.</p>

E2: Complete Statewide Security Policies, Standards and Procedures

Findings Summary	Deficient and absent security policies, procedures and processes — The State-supported framework for Security Policies and Procedures has gaps and requires resources for completion.
Corrective Action	Build upon the Spring 2003 “Gap Analysis” to complete the <i>Security Policies and Procedures</i> . This document will provide baseline security policies, standards and procedures across the State. The State should employ professional security experts to complete the statewide security standards, and should begin with the areas of the framework that are most in need of attention (see Appendix D for Policy Gap Analysis Summary).
Benefit	Without tailored policies, the State cannot effectively define or manage and maintain its security efforts. Providing a complete statewide framework for PSPs will enable the agencies to accelerate the development of agency-specific PSPs by using the template as a launch pad. A common core of PSPs will enable better assurance of quality, and tailoring will address unique agency environments and requirements.
Estimated Cost	Total one-time costs: \$387,000 Total annual recurring costs: \$35,000

E3: Improve Security Awareness and Training

Findings Summary	<p>Security expertise is lacking — Training of both security staff and end users is inadequate, overall. This situation may lead to security exposures and breaches due to a lack of knowledge around emergent issues and technologies, ability to identify issues, etc. In many cases, staff performing security roles are not trained to provide the protection required by the State and are therefore not fully equipped to address an agency's specific security requirements.</p>
Corrective Action	<p>Key actions are:</p> <ul style="list-style-type: none"> ■ Purchase and deploy the ISO 17799 standard to all agencies ■ Implement an enterprise-level security awareness program ■ Implement a centralized security training curriculum ■ Develop an evergreening process for training <p>Security awareness and security training are areas where the State can achieve significant economies of scale. Regardless of whether the State decides to develop its own programs or hires an external provider, the sheer magnitude of the effort for all of the agencies will position the State to achieve volume discounts above and beyond what any individual agency could achieve.</p> <p>It should be noted that the centralization of an awareness and training program would never meet all of the requirements of every agency. Agencies should continue to establish agency-specific processes and training for specific situations.</p>
Benefit	<p>Effective security training will reduce the overall costs of security incidents and improve security by:</p> <ul style="list-style-type: none"> ■ Reducing the number of exposures through better preparation and reduction in human error ■ Reducing the effect of incidents through rapid and more-effective response ■ Better use of resources <p>Implementing a security program at the State level will ensure that all of the training can be tailored to the State's approved policies.</p>
Estimated Cost	<p>Total one-time costs: \$504,000 Total annual recurring costs: \$205,000</p>

E4: Plan and Manage the Business Continuity Planning Efforts

Findings Summary	<p>Poor Risk and Business Continuity Management — Agencies lack basic disaster recovery processes and tools, including identification of key risk, recovery plans, recovery sites, staffing, etc. Most agencies, in the event of a disaster (fire, flood, electrical outage, etc.), have no realistic means to recover quickly from a technology disaster. This lack of disaster recovery preparedness potentially exposes citizens to the significant loss of services in case of a disaster. As the State increases its dependence on technology and extends its services to its constituents via technology, this issue will only grow.</p>
Corrective Action	<p>Develop an effective Business Continuity and Disaster Recovery Strategy and assist agencies to develop Disaster Recovery (DR) plans.</p> <ul style="list-style-type: none"> ■ Continue to train dedicated staff in Risk Management concepts, techniques and strategies. ■ Leverage the Business Impact Assessment tool to help each agency understand its risks and what assets need to be protected ■ Assist in conducting a Business Impact Analysis at each agency ■ Using the already purchased Strohl software, develop/enhance Standard Disaster Recovery plans ■ After the Business Impact Analysis, the State should consider an analysis of the most effective and efficient long-term disaster recovery strategy ■ Implement Business Continuity and Disaster Recovery strategies identified
Benefit	<p>Taking advantage of the fact that, in many cases, the recovery solution is substantially the same for similar disaster situations, a template can offer agencies some guidance in appropriate recovery plans, thereby saving many agencies the time necessary to discover, consider, plan and procure recovery options.</p> <p>Additionally, by centralizing the planning efforts, the State can take advantage of economies of scale in the implementation of hot-sites and other recovery solutions.</p>
Estimated Cost	<p>Enterprise Security Program Office one-time costs: \$2,033,000 Total annual recurring costs: \$1,308,000</p> <p>Calculation of the annual recurring costs: 0.20% of Operating Budget or a total of \$18,208,000, an increase of \$13,079,000 over the current amount spent by the agencies plus Enterprise</p>

Statewide Security Assessment Summary Report

Version No. FV01

May 2004

Security Programs, annually.

Total statewide spending target	\$18,208,000
---------------------------------	--------------

Current agency spending	<u>\$5,128,100</u>
-------------------------	--------------------

Total increase in spending to achieve target levels	\$13,079,000
---	--------------

Initial estimate for ongoing incremental allocation to the Enterprise Program for Business Continuity Planning and implementation should be 10 percent of the increase. This figure needs to be revised upon completion of the enterprise Business Continuity Planning process.

Agency-Level Recommendations

A1: Increase Funding to Agencies for Security

Findings Summary	Insufficient Funding for Agency Security Initiatives — The agencies do not have sufficient funding to sustain secure operations on a daily basis.													
Corrective Action	Each individual agency had areas in the assessment that required improvement. The additional funding included in this recommendation should be used by each agency for those improvements that the agencies feel are the best use of the funds to improve their specific agency posture.													
Benefit	The agencies have been in the position of trying to manage their security implementations with a severe lack of funding. This incremental funding should enable the State to dramatically improve its overall security posture, and thereby better protect the State’s information assets.													
Estimated Cost	<p>Total annual costs: 0.38% of Operating Budget or a total of \$34,595,000, an increase of \$20,759,000 over the current amount spent by the agencies plus Enterprise Security Programs, annually.</p> <table><tr><td>Total Statewide Spending Target</td><td>\$34,595,000</td></tr><tr><td>Current Agency Spending</td><td><u>\$14,016,000</u></td></tr><tr><td>Total Increase in Spending to achieve target levels</td><td>\$20,579,000</td></tr><tr><td colspan="2"> </td></tr><tr><td>Funding earmarked for other recommendations</td><td><u>\$5,382,000</u></td></tr><tr><td>Total annual incremental funding for agencies</td><td><u>\$15,197,000</u></td></tr></table>		Total Statewide Spending Target	\$34,595,000	Current Agency Spending	<u>\$14,016,000</u>	Total Increase in Spending to achieve target levels	\$20,579,000			Funding earmarked for other recommendations	<u>\$5,382,000</u>	Total annual incremental funding for agencies	<u>\$15,197,000</u>
Total Statewide Spending Target	\$34,595,000													
Current Agency Spending	<u>\$14,016,000</u>													
Total Increase in Spending to achieve target levels	\$20,579,000													
Funding earmarked for other recommendations	<u>\$5,382,000</u>													
Total annual incremental funding for agencies	<u>\$15,197,000</u>													

A2: Improve Agency Security Policies, Standards and Procedures

Findings Summary	<p>Deficient and Absent Security Policies, Procedures and Processes — Most State agencies have inadequate or nonexistent security policies and procedures. Many of the agencies currently default their security policy to the State-level Policy, Standards and Procedures, without any agency-specific tailoring. In some cases, however, the IRMC-approved standards and policies may not be detailed enough to meet agency specific-requirements.</p>
Corrective Action	<p>For agencies that require improvement in their policies, they should begin their development using the IRMC Policy framework as their baseline, and should be required to document each area individually where they default to the State-level security policies. Building upon that baseline, each agency should evaluate which policies need to be tailored to the agency's specific needs.</p> <p>Once developed, a central repository of all PSPs that are agency-specific should be created to allow reuse of notable best practices across the State. This repository should be used to promote sharing of best practices across agencies, and should be a simple document-management solution.</p> <p>Upon completing the policies, agencies are responsible for developing their own detailed procedures for day-to-day implementation of these policies.</p>
Benefit	<p>Without tailored policies, agencies cannot effectively define or manage and maintain their security efforts. A lack of detailed security procedures leaves an agency open to losing valuable intellectual capital in the event that a resource resigns. The statewide PSP framework will enable the agencies to accelerate the development of agency-specific PSPs by using the template as a launch pad. A common core of PSPs will enable better assurance of quality, and tailoring will address unique agency environments and requirements.</p>
Estimated Cost	<p>Total one-time costs: \$1,542,000 Total annual recurring costs: \$364,000</p>

A3: Increase Level of Security Staffing

Findings Summary	<p>Insufficient Levels of Staffing — A large majority of agencies have too few security staff or do not have staff dedicated to security. This deficit leads to confusion as to who is ultimately responsible for maintaining a secure environment, or for managing security events. Without appropriate levels of staff and appropriate skillsets, agencies cannot provide sufficient security on a consistent basis, address emergent issues, identify gaps or intrusions, and cannot defend against threats.</p>								
Corrective Action	<p>Ensure appropriate security staffing for each agency and, for smaller agencies, build a centralized pool of resources that can be deployed as necessary. To ensure that an appropriate level of attention is paid to security-related tasks, agencies need to employ staff that are fully responsible for security as part of their jobs.</p> <p>For larger agencies, regardless of the number of employees who are responsible for security, the organizational structure should conform to the roles defined by IRMC. For smaller agencies, a reduced number of individuals should share the roles. As an alternative, small agencies can participate in a shared services security program.</p> <p>While the decisions to employ full-time resources or external consultants lies directly with each agency, there are significant benefits to engaging outside consultants to perform activities that are one-time activities, or that require specific or specialized skills.</p>								
Benefit	<p>Ensuring assigned, designated, trained and staffed security roles helps ensure that critical aspects of security are covered. This includes the ability to mitigate emergent threats, develop new policies, identify key technologies, etc. With effective staffing and training, the State can address issues before they become threats and react quickly to threats.</p>								
Estimated Cost	<p>Gartner recommends that the State consider a shared service organization for the smaller agencies, to reduce the overall cost of supporting the smaller agencies' security requirements.</p> <table border="0"> <tr> <td>Total one-time costs:</td> <td align="right">\$2,145,000</td> </tr> <tr> <td>Total annual recurring costs:</td> <td align="right">\$2,145,000</td> </tr> </table> <p>Alternative: Hire individual security professionals at each agency</p> <table border="0"> <tr> <td>Total one-time costs:</td> <td align="right">\$3,080,000</td> </tr> <tr> <td>Total annual recurring costs:</td> <td align="right">\$3,080,000</td> </tr> </table>	Total one-time costs:	\$2,145,000	Total annual recurring costs:	\$2,145,000	Total one-time costs:	\$3,080,000	Total annual recurring costs:	\$3,080,000
Total one-time costs:	\$2,145,000								
Total annual recurring costs:	\$2,145,000								
Total one-time costs:	\$3,080,000								
Total annual recurring costs:	\$3,080,000								

A4: Improve Security Awareness and Training

Findings Summary	<p>Security Expertise Is Lacking — Training of both security staff and end users is inadequate, overall. This situation may lead to security exposures and breaches due to a lack of knowledge around emergent issues and technologies, ability to identify issues, etc. In many cases, staff performing security roles are not trained to provide the protection required by the State and are therefore not fully equipped to address an agency's specific security requirements.</p>
Corrective Action	<p>Key actions are:</p> <ul style="list-style-type: none"> ■ Implement security training and a training budget for key staff and users, including professional courses and certification ■ Develop an evergreening process for training ■ Develop a new-hire and refresher security training program <p>Once the curriculum has been developed by the Enterprise Security Program, the agencies need to review the materials and, where appropriate, tailor the training to the agency's specific requirements.</p> <p>It should be noted that the centralization of an awareness and training program will never meet all of the requirements of every agency. Agencies should continue to establish agency-specific processes and training for specific situations. Agencies can utilize templates and approaches of the centralized training program.</p>
Benefit	<p>Effective security training will reduce the overall costs of security incidents and improve security by:</p> <ul style="list-style-type: none"> ■ Reducing the number of exposures through better preparation and reduction in human error ■ Reducing the effect of incidents through rapid and more-effective response ■ Better use of resources <p>Implementing a security program at the State level will ensure that all of the training can begin with the State's approved policies.</p>
Estimated Cost	<p>Total one-time costs: \$431,000</p> <p>Total annual recurring costs: \$437,000</p>

A5: Replace Outdated Desktop Operating Systems

Findings Summary	<p>Outdated Desktop Operating Systems — Agencies are running desktops with obsolete operating systems (DOS, Windows 3.1, Windows 9x) that do not provide effective password or security protection. These insecure desktops expose the State network to intrusion and can expose confidential data.</p>
Corrective Action	<p>Upgrade 32,350 computers at the agencies to secure desktop operating system:</p> <ul style="list-style-type: none"> ■ 3,725 Windows 3.1 machines ■ 20,975 Windows 9x machines ■ 7,650 Windows 98 machines <p>In addition to the desktops described above, the latest inventory data shows that there are 5,400 Windows NT computers that are in use by the agencies. Despite the fact that these machines are not in compliance with the State's policy regarding the use of "N-1" operating systems, Gartner has not recommended that these machines be replaced, since Windows NT can be properly secured.</p>
Benefit	<p>Older operating systems cannot be properly secured. The immediate benefit of upgrading operating systems is to close known gaps in security, reducing security risks significantly.</p>
Estimated Cost	<p>Total one-time costs: \$38,820,000</p> <p>Hardware = \$700 Software = \$300 Installation = \$200 for 37,750 computers</p> <p>Gartner's research shows that properly managing desktops and maintaining relatively current desktops can reduce total cost of ownership of the desktop over the life of the equipment. Therefore, the costs to replace the machines may result in some additional savings that cannot be quantified without further analysis.</p>

A6: Improve Agency Border/Perimeter Defenses

<p>Findings Summary</p>	<p>Gaps in Agency Perimeter Defenses — The ITS organization within North Carolina operates the State network as an Internet Service Provider (ISP). However, many individual agencies control their own perimeters. These perimeters, though, are compromised by a lack of effective firewall technologies at many agency access points and/or improperly configured firewalls or outdated technology. Even secure areas of the State's network are exposed to intrusion due to trusted relationships with improperly secured parts of the network — a chain is only as strong as its weakest link.</p> <p>Many agencies' PCs have modems attached. Agencies should disable modems in computers that are able to connect to the State network, because it creates an unauthorized access tunnel to State systems.</p> <p>While a number of agencies explicitly forbid wireless networking or secure approved wireless networks, many do not. At many agencies there is no way to determine if active, unauthorized wireless devices (802.11, Bluetooth, etc.) are available.</p>
<p>Corrective Action</p>	<p>Purchase, upgrade, configure and install firewalls required to secure the State's computing resources.</p> <p>Close openings in perimeter as a result of modems and wireless setups</p> <ul style="list-style-type: none"> ■ Conduct detailed inventory of desktops, laptops and handheld devices, and ensure that any modems are properly disabled, and/or that modems and network connectivity cannot be enabled at the same time ■ Implement and monitor a policy that strictly forbids purchasing any new hardware with modems ■ Perform regular scans to detect rogue wireless networks and to ensure, for approved wireless networking, that appropriate encryption technology is implemented
<p>Benefit</p>	<p>Firewalls: Proper implementation can protect the State and agencies from attack, enable monitoring, and assist in preventing security-related events.</p> <p>Modems: By ensuring that no one computer can be connected to both the State network and an external network, the State can close a known gap in security.</p> <p>Wireless: By scanning for wireless networks, the State addresses an easily implemented rogue technology. Through appropriate encryption, the State</p>

	mitigates the risk of wireless network hijacking.
Estimated Cost	Total one-time costs: \$1,545,000 Total annual recurring costs: \$375,000

A7: Improve Risk Management and Update Business Continuity Plans

Findings Summary	Poor Risk and Business Continuity Management — Agencies lack basic disaster recovery processes and tools, including identification of key risk, recovery plans, recovery sites, staffing, etc. Most agencies, in the event of a disaster (fire, flood, electrical outage, etc.), have no realistic means to recover quickly from a disaster. This lack of disaster recovery preparedness potentially exposes citizens to the significant loss of services in case of a disaster. As the State increases its dependence on technology and extends its services to its constituents via technology, this issue will only grow.
Corrective Action	<p>Develop an effective Business Continuity and Disaster Recovery Strategy and develop a Disaster Recovery (DR) plan to protect agencies.</p> <ul style="list-style-type: none"> ■ Continue to train dedicated staff in Risk Management concepts, techniques and strategies ■ Conduct a Business Impact Analysis at each agency ■ Using the already purchased Strohl software, develop/enhance Standard Disaster Recovery plans ■ Smaller agencies should pool their resources and develop a shared-service data storage and retention strategy, so that each agency does not bear the entire cost of off-site storage ■ Larger agencies should seek community pricing based on volume for DR services providers, archival and data storage, etc. ■ Implement recovery strategies identified in the planning efforts
Benefit	Taking advantage of the fact that, in many cases, the recovery solution is the same or substantially similar for similar disaster situations, a template can offer agencies some guidance in appropriate recovery plans, thereby saving many agencies the time necessary to discover, consider, plan and procure recovery options.
Estimated Cost	<p>Total one-time cost (agency-level): \$3,467,000 Total annual recurring costs (agency-level): \$11,772,000</p> <p>These figures are based on a 10%/90% split between Enterprise-level and</p>

Statewide Security Assessment Summary Report

Version No. FV01

May 2004

Agency-level funding for this recommendation (total amount of \$13,079,000 as outlined in Recommendation E4). Allocation of BCP funding needs to be evaluated based on the outcome of the initial recovery planning efforts to account for a greater or lesser centralization of the recovery processes.

3. Detailed Statewide Security Recommendations

Based upon the assessment findings, several corrective actions have been recommended to improve the State's information security posture. These corrective actions are outlined in more detail below.

E1: Enhance the Enterprise-Level Security Program

The State should increase the funding to enhance the enterprise-level security program so that it is more in line with State and agency security needs. This enhanced program would formalize ongoing efforts; it would enable the State to address security threats and compliance levels at an enterprise-wide level; and it would assist individual agencies to develop security programs specific to their needs. A key component of this program would be to fund, budget and track security-related expenditures. In any multi-disciplinary organization there is a struggle between which functions should be centralized and which should be decentralized.

Thus, the State should consider taking the following short-term actions:

- Establish the appropriate governance mechanism for allocating and managing any additional funding that may be available. This activity should include proper investment management practices that ensure proper project selection, controlling and evaluating.
- Work with appropriate organizational authorities and define a formal security road map or strategy to address statewide security needs identified in this report. This road map should incorporate the ongoing self-assessments of the agencies on a yearly basis, as well as a statewide reassessment every three years. The road map should be tiered into statewide process/initiatives, common technologies and agency-specific requirements. The road map should address process, technology, governance and metrics.
- Translate the security road map into distinct projects or initiatives and prioritize them.
- Commit appropriate resources to the execution of defined security initiatives.
- Develop accounting mechanisms to budget and track information security expenditures at the individual agency and aggregate State level.
- Develop performance and improvement metrics for the State level and agency level to ensure that agencies are prioritizing security appropriately.

The State should also consider the following longer-term strategies to ensure ongoing improvement in the State's security posture:

- Work with procurement to develop means to make the selection of qualified vendors more expedient for the agencies.
- Establish a process to allocate funds for security enhancements, which includes the participation of the Office of the Controller, the Office of Budget and Management and the Enterprise Security Program Office. This strategy offers the benefit of giving an agency the authority to select which security activities and projects it will undertake to improve security. It also gives the Enterprise Security Program Office the responsibility to monitor the funds, to track utilization, and measure success to ensure that the additional funding is used to

improve the security profile of the agency. The rationale for centralizing the management of the security-related funds is to ensure that the security funds are not pooled with other agency program funds — which could then be reallocated to agency activities other than security. These funds could be used for purchases, training, audits (regardless of who conducts the audit), etc.

- Working with the agencies, establish standards for networking assets and configurations. The benefit of centralizing this effort is that the State will be able to take advantage of the procurement economies of scale as well as the benefits associated with a reduction of Total Cost of Ownership (TCO) realized when assets are standardized. (See discussion below.)
- Establish Enterprise-level purchasing programs for security-related components. These purchasing programs should aggregate demand across agencies and, on a regular basis, work with the vendor community (via appropriate procurement mechanisms for North Carolina) to provide the benefits of volume purchasing.
- The State should centralize monitoring for rogue wireless implementations. The number of agencies in the State that authorize the use of wireless is relatively small, yet a large number of agencies that prohibit wireless technologies never monitor for their usage. Centralized monitoring will enable the State to ensure that the network is protected, without requiring that individual agencies bear the costs of the technologies and training necessary to provide that protection.
- Ensuring a continuous level of appropriate security through regular enterprisewide and agency-level assessment. It is recommended that the State conduct an expert security assessment every three to five years. The State may wish to implement this on a staggered basis, so that one-third of the agencies are assessed annually and a complete cycle is completed every three years. These ongoing assessments would enable the State to track how effectively its security program meets requirements, identify progress to goal, address any gaps in a timely fashion, as well as generate information required for strategic and tactical enhancements to State and agency-level efforts. In addition, each of the State agencies should develop periodic self-assessment program to track progress. In order to meet the legal requirements of the State, each agency should be required to conduct a self-assessment, annually, that describes its progress in improving its security posture with the increased funding available to it. The agencies should submit their self-assessment to the Enterprise Security Program Office in order to comply with the legal requirement for the CIO to submit a summary to the Legislature on January 15th of each year.

Standardize Network Assets and Configurations

The State of North Carolina should establish standards for network assets and configurations across the State, and the Enterprise Security Program Office should establish security standards for those assets and configurations. Presently, the State and agencies have numerous networks using disparate technologies, processes, architectures, etc. This heterogeneous environment is far more difficult to secure and manage due to its greater complexity.

Standardizing could include:

1. Standard network topologies
2. Preferred hardware and software vendor lists

3. Qualified security vendors
4. Network security assurance testing and validation processes
5. Approved network protocols
6. Approved encryption and remote access methods, etc.

Standardized assets allows improved centralized monitoring and management of assets through automated management programs (such as Ciscoworks or OpenView), which creates a more holistic network security process. Additionally there is evidence of a lower total cost of ownership on standardized assets, including the ability to properly train employees on the technologies.

Standardization, in general, will also reduce system downtime in the event of a disaster recovery scenario.

Additionally, qualified and authorized network administrators could perform peer reviews across State agencies to assist in spotting potential vulnerabilities. This aspect of the recommendation assumes that the State is interested in breaking down any barriers that are inherent in multi-agency organizations.

E2: Develop and Maintain Statewide Policy, Standards and Procedures (PSPs)

The State should continue to build upon the work identified by the Gap Analysis and should finalize the State PSP framework. On completion, the State should establish a program to assist agencies in tailoring the State framework to meet their own requirements. The program should be funded at the State level, and should engage experts in establishing security policy, standards and procedures. In this way, the State can ensure that all agencies have a common baseline of security PSPs.

Once agency-specific PSPs are developed, agencies must review and update them annually to meet changing technology and government requirements. To do so, the State should designate and fund a pool of technical writers. Technical writers can ensure that the individual agency's PSPs documentation is kept up-to-date, that it follows statewide best practices and adheres to consistent standards and measures.

Upon completion of the development of the PSPs, each agency should develop a process of evergreening to ensure that the PSPs stay current and relevant.

E3: Implement Formal Security Training and Awareness Program

A formal security training and awareness program should be developed. A key component of the training program is a process to provide appropriate levels of information security training for staff directly responsible for security, as well as certify the skills of the staff. Security staff should be tiered based on duties and responsibility and provided with commensurate hours of training

per year. Such training should focus on developing specialized skills in relevant technologies and techniques that will improve agencies' security postures.

A user security and awareness training program will assist State agencies in preserving the confidentiality, integrity and availability of agency information resources. In order to protect agency information and systems, security awareness must be supported and policies adhered to by all levels within the State. Users who do not receive appropriate training are unlikely to understand the importance of information security and the need to comply with information security policies. Key to an effective end-use security program is ensuring that:

1. All new hires receive security training on orientation
2. Any resources transferring from other agencies go through training
3. Refresher training be provided on an annual basis as a component of annual employee training
4. Security "marketing" efforts that include daily reminders for end users (e.g., posters, bookmarks, notices on employee pay stubs)

As with the statewide PSP framework, the Enterprise Security Program Office should create base-level awareness program and design recommended training requirements. Additionally, it should then act as a repository for agency-specific training and awareness curricula and assess follow-through with the efforts. For smaller agencies, Gartner would recommend that the State establish a shared-services training effort that is managed centrally.

E4: Improvement Risk Management and Update Business Continuity Plans

An initiative should be undertaken to build upon the existing business continuity planning effort to extend contingency planning to address all critical State agency processes (such that IT systems disaster recovery forms a component of business continuity planning). Key corrective action steps to consider are:

- A statewide Business Impact Analysis project should be undertaken which looks at each agency individually and rolls the needs of each agency into a statewide position. The goal is to prioritize the critical needs of the State as a whole, across agencies. Lessons learned from the Y2K initiative, as well as Sept. 11, should be incorporated into the BIA program.
- The Business Impact Analyses of the agencies should be analyzed to ensure that the relative impact of an outage on an agency is appropriately prioritized, in comparison to other agencies. For example, what is identified as absolutely mission-critical to one agency may be less important to the State, as a whole, than an application or a process at another agency. Additional economies of scale could be identified so that funds are not expended on redundant recovery efforts.
- Agencies should form a consortium to pool resources to support one another to respond to adverse events.
- Resumption procedures need to be developed that describe the actions required to return to normal business operation mode.

- A variety of testing techniques should be specified to increase the likelihood of plans succeeding in real-life situations. These may include, but are not limited to, tabletop testing, simulations, technical recovery testing, test recovery at alternate site(s), test of supplier facilities and services, and complete rehearsals.

Maintenance procedures should be included within an existing, formal change management program to ensure that timely updates are made, and that such modifications are subjected to appropriate controls.

4. Detailed Agency-Level Security Recommendations

A1: Increase Funding to Agencies for Security

On average, North Carolina State agencies spend approximately 0.15 percent, on average, for security. That percentage is less than one-half the industry average of 0.38 percent. Gartner recommends that the State increase the overall funding for information security. In early years, the increase may be higher due to a need for investment to meet minimum requirements. Once these “capital” investments are made, the later operational expenses may decline as maintenance levels are achieved.

A2: Develop and Maintain Agency Policy, Standards and Procedures (PSPs)

Agencies should tailor the State-level PSPs to support agency-specific requirements.

An important point to note is that the detailed procedures necessary to implement the policies are as important as the policies themselves. Many agencies had policies but had never operationalized them to support the day-to-day management of the agency security program. These procedures are the only sure way that an agency can ensure that the security activities are performed consistently.

Once agency-specific PSPs are developed, agencies must review and update them annually to meet changing technology and government requirements. To do so, the State should designate and fund a pool of technical writers. Technical writers can ensure that the individual agency's PSPs documentation is kept up-to-date, that it follows statewide best practices and adheres to consistent standards and measures.

Upon completion of the development of the PSPs, each agency should develop a process of evergreening to ensure that the PSPs stay current and relevant.

A3: Increase Level of Security Staffing

Agencies need to be funded to increase the security skills of their personnel. Virtually all agencies' assessments identified the need for additional resources.

To ensure that an appropriate level of attention is paid to security-related tasks, agencies need to employ staff that are fully responsible for security as part of their jobs.

For large agencies, an increase of two full-time internal resources is appropriate. The staffing should — at a minimum — conform to the three roles defined by IRMC. This level of staffing is estimated based on the amount of work necessary to bring the large agencies to a reasonably solid security posture and then to maintain that level.

For medium-size agencies, one full-time resource should be added, where appropriate. There are several medium-size agencies where resources were not an issue.

For smaller agencies, one option is to hire full-time resources, which is often deemed as excessive, based on the size of the agency. Alternatively, the smaller agencies could build a centralized pool of resources that can be deployed as necessary.

While the decisions to employ full-time resources or external consultants lies directly with each agency, there are significant benefits to engaging outside consultants to perform activities that are one-time activities, or that require specific or specialized skills.

A4: Implement Formal Security Training and Awareness Program

A formal security training and awareness program should be developed. A key component of the training program is a process to provide appropriate levels of training for staff directly responsible for security, as well as certify the skills of the staff. Security staff should be tiered based on duties and responsibility and provided with commensurate hours of training per year. Such training should focus on developing specialized skills in relevant technologies and techniques that will improve agencies' security postures.

A user security and awareness training program will assist agencies in preserving the confidentiality, integrity and availability of agency information resources. In order to protect agency information and systems, security awareness must be supported and policies adhered to by all levels within the State. Users who do not receive appropriate training are unlikely to understand the importance of information security and the need to comply with information security policies. Key to an effective end-use security program is ensuring that:

- All new hires receive security training on orientation
- Any resources transferring from other agencies go through training
- Refresher training be provided on an annual basis as a component of annual employee training
- Security "marketing" efforts that include daily reminders for end users (e.g., posters, bookmarks, notices on employee pay stubs)

As with the statewide PSP framework, the Enterprise Security Program Office should create a base-level awareness program and design recommended training requirements. Agencies should be required to build upon the State-level program to accommodate agency-specific requirements.

A5: Replace Outdated Desktop Operating Systems

State agencies need to upgrade the desktop environment to the latest secure operating system. As identified in the Opportunities for Improvement, the State has a large number of obsolete, insecure desktop operating systems. These desktop operating systems need to be upgraded rapidly. Upgrading, in many cases, will involve not just the system software, but also the PC applications and hardware.

A key success driver is validating the desktop inventory already conducted to ascertain the total scope of exposure, and to provide a clear foundation for vendor volume negotiations. Aggregated purchases and deployment can significantly reduce the initial investment requirements on an agency-by-agency basis. A secured desktop environment will decrease the risk of unauthorized access to systems and data. The hardware vendors should conduct training on the support and maintenance of the machines to ensure that all of the security options embedded into the machines and operating systems are enabled.

If possible, the State should establish a set of standard configurations that includes appropriate virus protection, security configurations, password requirements, etc., that can be pre-installed by the desktop vendors. This practice could significantly reduce the total cost of ownership of the new machines that are purchased, and may help offset the initial cash outlay.

A6: Improve Agency Border/Perimeter Defense

An agency's border/perimeter is the virtual boundary that separates the agency network from the public networks. There are many access points in a border/perimeter. Included in this recommendation are three core components that required remedial attention: Firewalls, Modems and Wireless.

Firewalls

State agencies should install firewalls in order to protect remote facilities, as appropriate. This would improve confidence in the security of the entire network. Wherever possible, firewalls can be aggregated. Firewalls deployed around the State can be centrally managed via secure channel connections such as VPN (Virtual Private Network) or SSL (Secure Sockets Layer) technologies at each firewall. The firewalls must be maintained with a tightly controlled configuration standard.

Proper perimeter defense would block unauthorized access to the information and information resources contained in the facility. Firewall configurations and regular monitoring of logs will help to identify and block potentially dangerous events.

Modems

All modems in use, or available on desktops and laptops, should be inventoried and documented. Desktop modems should be removed to eliminate a potentially insecure communication channel into the network — this will require a statewide inventory of personal computers. Unless there is a requirement for a specific modem, it should be removed. Very few agencies reported having modems remaining in PCs, so this recommendation is intended to close the last remaining gaps.

In the event that the modem is required for business-related reasons, the desktop should be configured so that the modem and the network capabilities are not enabled at the same time, thereby protecting the internal network from potential exposure to unwanted access.

Wireless

While wireless networking use is minimal at the State, there is growing popularity, and it is very simple to add wireless capabilities to a computer.

Agencies need to implement and adhere to the statewide standard for wireless, as well as develop and implement their own detailed procedures for implementation.

Regardless of whether agencies permit wireless networking, a process of scanning for wireless networks must be implemented at the State. This scanning would serve two purposes:

1. Ensure the approved networks are properly secured
2. Assess whether any unauthorized wireless networks have been implemented

A7: Improvement Risk Management and Update Business Continuity Plans

An initiative should be undertaken to build upon the existing business continuity planning effort to extend contingency planning to address all critical State agency processes (such that IT systems disaster recovery forms a component of business continuity planning). Key corrective action steps to consider are:

- A statewide Business Impact Analysis (BIA) project should be undertaken, which looks at each agency individually and rolls the needs of each agency into a statewide position. The goal is to prioritize the critical needs of the State as a whole, across agencies. Lessons learned from the Y2K initiative, as well as Sept. 11, should be incorporated into the BIA program.
- The Business Impact Analyses of the agencies should be analyzed to ensure that the relative impact of an outage on an agency is appropriately prioritized, in comparison to other agencies. For example, what is identified as absolutely mission-critical to one agency may be less important to the State, as a whole, than an application or a process at another agency. Additional economies of scale could be identified so that funds are not expended on redundant recovery efforts.
- Agencies should form a consortium to pool resources to support one another to respond to adverse events.
- Resumption procedures need to be developed that describe the actions required to return to normal business operations mode.
- A variety of testing techniques should be specified to increase the likelihood of plans succeeding in real-life situations. These may include, but are not limited to, tabletop testing, simulations, technical recovery testing, test recovery at alternate site(s), test of supplier facilities and services, and complete rehearsals.

Maintenance procedures should be included within an existing, formal change management program to ensure that timely updates are made with appropriate controls.

Additional Recommendations for Agencies

Incorporate Security Reviews into the Application Development Life Cycle

Automated business systems should include periodic security reviews from the initial design phase through operational implementation. The extent of these reviews is dependent on the criticality and complexity of each application.

Such a methodology should ensure tight integration of security principles at each stage of the application development life cycle. The initial stages of the new or large-scale development efforts (especially the Analysis, Design and Construction) should involve providing security input in an advisory role to the development process. This would help to ensure that the application is developed with security principles in mind and will minimize the possibility of major structural changes that may be needed if serious issues are discovered as part of the review and testing process. The last two phases (Testing and Rollout) should involve the actual security review and testing process.

Application security reviews and tight integration of security during all phases of development will help ensure that:

- Security flaws in the application architecture or embedded within the design do not go unnoticed
- Application design takes place with a clear focus on security principles
- The possibility is minimized that major structural changes may be needed in case serious issues are discovered as part of the review and testing process

Standardize Network Assets and Configurations

Standardize configurations within State agencies based on a consistent set of guidelines. Presently, the agencies have numerous networks using disparate technologies, processes, architectures, etc. This heterogeneous environment is far more difficult to secure and manage, due to its greater complexity.

Standardizing would include:

1. Server/firewall “build sheets”
2. Audit settings
3. Backup procedures

Standardization, in general, will also reduce system downtime in the event of a disaster recovery scenario, since recovery would be streamlined.

Fully Automate Antivirus Management

Despite the successes realized by the State, automated antivirus management should be considered. Gartner does not recommend that the State standardize on any single antivirus software, but rather that the State continue to diversify the products in use, to ensure that a maximum level of protection is achieved. The automation of the updates, however, can more quickly close the gaps, once identified.

Additionally, as the State extends its e-government efforts, antivirus complexity and requirements will increase. Without the addition of automated processes, it will be more difficult to assure antivirus protection going forward.

Implement Comprehensive Logging

Unauthorized access will go undetected unless internal audit logs are monitored consistently. If, as is the case in most agencies, logs are not monitored, agencies may experience excessive preventable attempts to gain access to systems.

State agencies should implement comprehensive logging on all critical systems, especially systems with access from outside networks. Agencies should regularly review logs for security events and anomalies that may indicate a system has been compromised — critical systems should have their logs reviewed daily. This action would significantly increase the chance of detecting stealth attempts to compromise systems, and significantly shorten recovery time in the event that a system is compromised and manipulated. Without sufficient logging, detecting and recovering from a sophisticated attack can require considerable resources and may extend network outages.

Automated tools should be evaluated to consolidate cross-platform systems and application logs. This will decrease the amount of time spent gathering and monitoring logs. In some instances, the State may need to hire additional staff to maintain proactive monitoring. External service providers should be considered as well, to provide for 24×7 monitoring. In general, logs should be activated on all critical systems and proactively monitored.

Improve Information Classification

Many of the agencies do not have information classification PSPs. Many agencies take the perspective that all of the data is public and, in some cases, voiced strong opposition to needing high levels of security, since “their data was not confidential”. Protecting data from inadvertent release to the public is only one aspect of security. Protecting the data from being changed by unauthorized access is of greater importance; since altered data can severely undermine the public’s confidence in government. While records may be public, most agencies may wish to initially restrict access for works-in-progress, policy drafts, etc. At a minimum, all agencies without information classification policies should adopt IRMC’s Data Handling Policy and tailor it for their specific use.

By classifying information according to its security requirements, defining how that data needs to be treated, and how they should be disposed, the agencies will be positioned effectively to manage and protect information.

Utilize Encryption Technologies

While the result of this study found that there is not currently a pressing need for wide deployment of encryption technologies, encryption technology use is on the rise. State agencies should utilize encryption technologies whenever appropriate, e.g., mobile communications, remote access, wireless networking, personal computer disk drives, etc. The use of encryption technologies throughout the agencies will safeguard the integrity and confidentiality of the critical agency information assets. In order to ensure interoperability, agencies should follow the encryption architecture defined by the State.

Establish a Security Handbook

State agencies should develop and implement a security handbook. A security handbook extracts key, salient points from the more detailed security PSPs, and can take the form of a physical book, an online Web site or other medium. The purpose of the security handbook is to be a quick reference tool for staff, outlining the basic security requirements of the agency. The security document should include an employee acknowledgement form. Streamlined security policies documentation and signed acknowledgements will ensure that employees are provided with more-focused instruction on security requirements. This increases the effectiveness of policy communication processes.

5. Detailed Security Findings by ISO 17799 Category

This section expands upon the findings and recommendations presented previously. It includes additional notable practices and opportunities for improvements based upon the ten ISO 17799 categories contained in the assessment.

Items identified as **Notable Practices** are items that provide effective security. Only Notable Practices that affect a majority of agencies are presented below. The diverse implementation of security practices across the agencies means that only a few notable, statewide practices exist.

Similarly, items identified as **Opportunities for Improvement** are items that impair State security. Only Opportunities for Improvement that affect a majority of agencies are presented below.

1. Security Policies, Standards and Procedures (PSPs)

Security Policies, Standards and Procedures address management support, commitment and direction in accomplishing information security goals.

Key findings related to Security Policies, Standards and Procedures include:

Notable Practices

- State-level security PSPs are largely in place and, where possible, are used as a basis for developing agency-specific PSPs and guidelines.
- In order to provide security management oversight, many agencies have created some form of internal security oversight committee. This forum has buy-in from senior-level management and is comprised of the division management. It allows the agencies to take input from the various divisions, draft standards and policies, and to ensure the widest possible dissemination.
- Most of the agency-specific policies make clear the consequences of non-compliance.

Opportunities for Improvement

- Few employee information security handbooks exist. The absence of these documents fosters a lack of guidance among the user community and may contribute to employees engaging in poor security practices, e.g., leaving written passwords in their work areas.
- Most agencies' PSPs are not tailored to agency requirements. Typically, the standards and procedures default to the IRMC PSPs. Additionally, many procedures are *ad hoc* in implementation and enforcement.
- Few regular, formal management-reporting processes occur regarding security compliance. Informal, non-technical reporting takes part on an *ad hoc* basis as issues or needs arise.
- Less than 30 percent of the agencies have procedures in place to keep the policies up-to-date.

2. Organizational Security

Organizational Security addresses the need for a management framework that creates, sustains and manages the security infrastructure.

Key findings related to Organizational Security include:

Notable Practices

- Agencies are actively working to develop formal security organizations.
- Most agencies have named security owners.

Opportunities for Improvement

- With one exception, information security programs do not receive a line item in the budget. Without a security line item, it is difficult to track security expenditures and efforts. Additionally, during a management change, lack of security budgeting confuses understanding of the ongoing security efforts. The State should add an account code specifically for security-related expenditures.
- Few agencies track security metrics.
- Current security positions within the organization are insufficiently staffed to meet most agency-stated requirements. Current security administrators split their time between administrative and security duties, preventing them from spending enough time on information security issues. This greatly increases the likelihood of an exposed vulnerability and increases the possibility that State confidential information could be exposed. Small agencies could mitigate much of this issue by either outsourcing for the skillsets or by pooling resources to enable them to fill the gaps.

3. Asset Classification and Control

Asset Classification and Control addresses the ability of the security infrastructure to protect organizational assets.

Key findings related to Asset Classification and Control include:

Notable Practices

- A large portion of the agencies have an asset inventory in place.

Opportunities for Improvement

- The information classification methodology is incomplete for most agencies. Security controls cannot be applied appropriately if a consistent information classification methodology is not followed. Additionally, a comprehensive information classification policy makes it much easier for the custodian of information to communicate to users the need for discretion when handling confidential data.
- Confidential hard-copy information is sometimes left on desks, printers and faxes, which could lead to a leakage of information.

- A predominance of agencies do not have an information-handling matrix that explains how specific information should be handled.

4. Personnel Security

Personnel Security addresses an organization's ability to mitigate risk inherent in human interactions.

Key findings related to Personnel Security include:

Notable Practices

- For many agencies, new employees, as well as contractors, are required to agree to and sign a confidentiality agreement. In addition, contractors or external parties are required to sign a nondisclosure agreement.
- For most agencies, when an employee is found not to be in compliance with security policies, appropriate disciplinary action is taken.
- Most employees are made aware of their responsibilities for protecting information resources and for securing physical assets.

Opportunities for Improvement

- A formal security roles and responsibilities document (e.g., charter) typically does not exist at the agency level. Daily security operations for implementing and maintaining security policy are at high risk when security roles and responsibilities are not defined.
- There are not sufficient resources at most agencies to achieve security goals. This includes hardware and software resources as well as sufficient manpower for the implementation and maintenance of the security infrastructure.
- Many audit logs and other reporting mechanisms are not regularly reviewed and are not in place on many systems. This can have a significant impact because it makes it very difficult to identify, remediate and prosecute a successful attack.
- Most agencies do not practice consistent screening of vendors and contractors. In many cases, requirements are established and implemented by an external hiring organization — not the agency. In some cases, agencies are relying on other agencies to do background checks and those checks are not being performed — which may lead an agency to be overconfident that the personnel being hired have cleared the background checks.
- Staff lacks an understanding of their roles and responsibilities in protecting information assets.
- Agencies lack an adequate security-training program that addresses individual staff duties and responsibilities appropriate to the staff role.
- Security-related responsibilities are not generally included in job descriptions of the end-user employees. The inclusion of security-related responsibilities would heighten the awareness of all employees, since the responsibilities will be discussed at least annually.
- Employees do not receive formal feedback related to their security responsibilities during their performance evaluations.

5. Physical Security

Physical Security addresses the risk inherent to organizational premises.

Key findings related to Physical Security include:

Notable Practices

- Most employees are aware of the appropriate practices that are necessary to protect their physical facilities — similar to an employee's understanding of the need to lock his/her own home. In addition, physical security practices such as visitor sign-in procedures are frequently employed.
- A predominance of the agencies had additional levels of controls for after-hours access to their facilities.
- A majority of the agencies adequately protect their hardware assets from theft.
- Keys and key cards are managed properly. Formal procedures exist in almost all agencies to ensure that access to locked facilities is managed.
- Many agencies have secure desktops, with users making the appropriate efforts to secure PC workstations when unattended, including after business hours.
- Off-premises equipment is inventoried, managed and protected.

Opportunities for Improvement

- Some data centers have a standard sprinkler system enabled for fire protection. Water will cause unnecessary damage to critical systems in the event of a contained fire or accidental sprinkler discharge.
- Computing equipment is not consistently disposed of in a secure manner. There is a chance that confidential data could be exposed to unauthorized individuals.
- There is no consistent handling and destruction of documents across the agencies.
- Physical security mechanisms at most agencies are not tested through a formal testing process; confirmation of their proper operation is only verified through ordinary day-to-day operations.
- Many agencies have old and outmoded desktop operating systems that lack built-in security mechanisms to appropriately secure agencies' networks.

6. Communications and Operations Management

Communications and Operations Management addresses an organization's ability to ensure the correct and secure operation of its assets.

Key findings related to Communications and Operations Management includes:

Notable Practices

- Statewide security policy was recently implemented requiring that all security incidents be reported to ITS. In addition, the agencies submit formal report and briefs.
- Agencies implement appropriate controls to mitigate the risks of computer viruses. The negative impacts caused by security viruses have been low over the last year, due to the application of effective controls.
- Test, development and operations facilities are adequately delineated and separated at most agencies.
- Overall, there is good security coordination between the agency and third-party providers.
- Multiple layers of security controls protect some agency e-commerce and Web resources, implying that agencies with Web applications tend to have a clearer understanding of the need to protect those systems.
- For remote access users, the employees are made aware of their specific responsibilities for keeping access codes secure.
- Electronic mail (e-mail) policies are clearly defined, communicated and enforced. The NCMAIL system used by agencies deploys effective technologies to protect e-mail.

Opportunities for Improvement

- Approved detailed operating policies and procedures are incomplete. The lack of complete operating procedures reduces the agencies' ability to prevent and recover from security incidents by allowing practices to vary between divisions within the agencies. The existence of varying practices complicates the process of detecting and recovering from security incidents.
- There is a lack of processes to certify security for new system implementations. There are some standards for software systems in place, but when the agency manages its own desktops, the patching and fixing of desktops is largely not controlled.
- Since the process is so new, agencies do not yet fully subscribe to the documented incident reporting and response procedures outlined in IRMC Policy 161, "Incident Management". In addition, there is a lack of documented investigative procedures. There are few documented operational plans for recovery from security incidents.
- Antivirus solutions, while multi-tiered and largely effective, depend mostly on end-user and manual processes for updating virus signatures. Despite this fact, the State has experienced very little loss as a result of virus attacks, indicating that the virus protection tends to be acceptable. Automating the updating of virus signatures could improve the virus protection at the State.

7a. Access Administration

Access Administration addresses the administrative aspects of an organization's ability to control access to assets based on business and security requirements.

Key findings related to Access Administration include:

Notable Practices

- Manager or supervisor approval is required as part of various user-access management procedures. Timely user access termination has also been assigned.
- Systems are checked to ensure guest and temporary accounts are disabled.
- Agencies use an automated process that prompts users to change their initial password upon first login, and many agencies take the steps to control critical systems through password protection.
- Almost all of the agencies remove unauthorized communication devices (e.g., modems) from PCs.
- Although not consistently tracked, access to the root-level system is largely controlled.

Opportunities for Improvement

- There is no consistent process for monitoring application logs. Failure to appropriately capture and monitor application logs may result in suspicious activity, or security events within the application, going unnoticed.
- Few of the agencies conduct periodic audits of user access to ensure that users have the appropriate levels of access and privilege.
- Very few agencies have any process to test passwords for strength and appropriateness. Ensuring that all passwords contain a mix of special characters, and are of a certain length, will enhance the State's ability to protect against certain types of attacks.
- There is significant risk due to the absence of PSPs regarding system access logging. This fact limits the probability of adequate security event monitoring, detection and/or tracking — as well as ensuring that investigations of events are hindered by the lack of adequate logs and monitoring.
- Most of the desktops in use lack the technology (e.g., obsolete operating systems and inadequate hardware) to provide logical security. This fact makes it difficult for agencies to secure access to local desktop systems. Ease of access to desktop systems thereby exposes the information stored on these systems, as well as computers connected to those systems. For example, a visitor to a site could simply reboot a Windows 3.1 system and would not be required to supply a password to gain access to the computer.

7b. Access Technology

Access Technology addresses the technological aspects of an organization's ability to control access to assets based on business and security requirements.

Key findings related to Access Technology include:

Notable Practices

- Many network administrators utilize industry-standard tools to perform their jobs.
- A majority of the network and system administrators have adequate experience to implement the security policies and procedures.

- For most agencies, a network diagram is available that adequately describes the agency environment. This fact helps ensure that the agency has a clear and accurate picture of the network to ensure changes and additions are made with security in mind.
- For agencies with firewalls in place, only approved protocols are permitted to pass through the firewall.

Opportunities for Improvement

- Firewalls and critical systems are not under 24×7 monitoring. With current levels of logging and monitoring, a compromised system would be very difficult to detect. Intrusions that occur after hours may be very difficult to investigate if detection is far after the event.
- There are insufficient policies across the agencies for defining the types of data that are permitted on mobile devices (e.g., laptops). This lack of definition may mean that confidential data is stored on machines that are more susceptible to theft.
- Critical system logs are not reviewed and reconciled on a regular basis. Without the review and reconciliation of logs, system abuse, security incidents and inappropriate use of rights could go undetected.
- While 13 agencies permit wireless implementations, when wireless is permitted, more than one-half of the agencies deploy without required security controls. The insecure networks are vulnerable to external threats, which could lead to the compromise of agencies' internal networks.
- Few agencies monitor for rogue wireless implementations. While some agency policies state that wireless is prohibited, monitoring at all agencies is required to ensure that employee or contractors do not inadvertently expose the agency to risk by simply installing a wireless hub for convenience purposes.
- Overall, there have been very few penetration tests performed, vulnerability assessments, or infrastructure audits performed. Untested firewalls, lack of penetration tests or audits can leave unknown holes in agency perimeters and could undermine an agency's ability to secure their network.

8. Applications Development and Maintenance

Applications Development and Maintenance addresses an organization's ability to ensure that appropriate information system applications security controls are both incorporated and maintained.

Key findings related to Applications Development and Maintenance include:

Notable Practices

- Most applications are built with security in mind and with the appropriate level of access controls.
- In a majority of the agencies, application libraries and source libraries are appropriately managed and controlled.

- Mainframe and distributed environments are typically separated into development, test and production environments, in order to protect the confidentiality, integrity and availability of production systems.
- Many agencies implement Web technology (i.e., secure socket layer [SSL] technology) on Web servers to ensure secure communication of confidential information.

Opportunities for Improvement

- Test data does not receive the same level of security protection as production data does. In addition to being segregated into its own logical network, development servers and test data should be secured with the same degree of protection.
- Test equipment needs to be brought to the same level of security as the production equipment.
- Less than one-half of agencies employ formal change control procedures.
- Less than one-half of the agencies test purchased software with the same rigor as applications developed in-house.

9. Business Impact/Continuity Management

Business Impact/Continuity Management addresses an organization's ability to counteract interruptions to normal operations.

Key findings related to Business Impact/Continuity Management include:

Notable Practices

- Many agencies have identified off-site storage facilities.
- Mainframe-hosted applications have hot-site storage contracts with defined restoration facilities. These restoration facilities are at a distance, which provides good confidence that they will not be affected by any disaster at the primary data center.
- Although most are aged, a large majority of the agencies were able to produce a copy of some sort of business continuity/disaster recovery (DR) plan. In many cases, these DR plans, however, have not been tested.

Opportunities for Improvement

- Overall, business continuity planning is not adequately addressed.
- Relevant personnel have not been trained in backup, recovery, crisis management or business continuity.
- Most of the agencies have not performed a business impact analysis in the recent past (i.e., since late 1990s in preparation for Year 2000).
- Agencies have not identified key disaster scenarios to aid in determining requisite recovery strategies. Agencies have not developed a disaster recovery (DR) plan based on different scenarios, taking into account regions, power availability, equipment acquisition for critical

applications and data, retrieval of critical data and restoration of public (data centric) services.

- Critical inventories to recover from a disaster are not in place — meaning that agencies may not have what is needed to recover from a catastrophic system loss.
- There have been limited efforts to conduct business impact/risk analysis for critical systems and establish a recovery time objective (RTO). The RTO identifies how quickly a system must be restored and back in production, and would enable the agency to determine the best possible business recovery alternative.
- Interdependencies between systems from a DR perspective have not been identified.
- Some agencies reported inadequate storage of DR plans, e.g., at employees' residences, DR sites, the affected location site, or in exposed systems. Storage of continuity plans at employees' residences is a serious risk to operational recovery.

10. Compliance

Compliance addresses an organization's ability to remain in compliance with regulatory, statutory, contractual and security requirements.

Key findings related to Compliance include:

Notable Practices

- Many agencies have policies that address appropriate legal matters including legislation, intellectual property rights and records retention.
- Appropriate protections for privacy and confidentiality are followed as required by applicable legislation.
- Access warning messages indicating appropriate use of data/system access are generally in use by the agencies.

Opportunities for Improvement

- Few compliance reviews of security policies or technical compliance checks (e.g., vulnerability test) have been performed.
- Few agencies conduct compliance audits to ensure adherence to agency records-retention policies.
- Compliance reviews of security policies or technical compliance checks have not been performed in the recent past.

6. Statewide Security Expenditure Summary

Figure 6: IT Security Expenditure as a Percentage of Operating Budget

Agency	FY 03–04 Agency Operating Budget	FY 03–04 IT Security Expenditure (Actual and Projected)	IT Security Exp. as % of Agency Operating Budget
Department of Administration	\$ 145,000,000	\$ 26,643	0.02%
Office of the Lieutenant Governor ⁵	\$ 601,722	\$ 7,973	1.33%
<i>Subtotal:</i>	<i>\$ 145,601,722</i>	<i>\$ 34,616</i>	<i>0.02%</i>
Department of Agriculture and Consumer Services	\$ 91,332,520	\$ 212,644	0.23%
Department of Commerce	\$ 1,069,772	\$ 41,531	3.88%
Department of Corrections	\$ 992,590,000	\$ 423,340	0.04%
Department of Crime Control and Public Safety	\$ 188,703,529	\$ 113,283	0.06%
Department of Cultural Resources	\$ 55,911,271	\$ 3,936	0.01%
Department of Environment and Natural Resources	\$ 290,355,198	\$ 270,999	0.09%
Department of Health and Human Services	\$ 3,225,850,216	\$ 2,671,705	0.08%
Department of Insurance	\$ 26,687,485	\$ 149,477	0.56%
Department of Justice	\$ 95,688,196	\$ 568,767	0.59%
Department of Juvenile Justice and Delinquency Prevention	\$ 132,180,585	\$ 184,411	0.14%
Department of Labor	\$ 27,019,036	\$ 211,616	0.78%
Department of Public Instruction	\$ 31,459,678	\$ 634,706	2.02%
Department of Revenue	\$ 76,200,000	\$ 1,134,069	1.49%
Department of State Treasurer	\$ 35,055,313	\$ 289,757	0.83%
Department of Transportation	\$ 3,247,069,755	\$ 579,137	0.02%
Employment Security Commission	\$ 161,465,750	\$ 426,343	0.26%
NC Community College System	\$ 34,442,728	\$ 11,000	0.03%
Office of Information Technology Services	\$ 147,652,207	\$ 5,674,350	3.84%
Office of the Governor ⁶	\$ 5,215,781	\$ 16,083	0.31%
<i>Subtotal:</i>	<i>\$ 152,867,988</i>	<i>\$ 5,690,433</i>	<i>3.72%</i>
Office of State Auditor	\$ 13,096,880	\$ 34,430	0.26%
Office of State Budget and Management	\$ 4,211,805	\$ 17,463	0.41%
Office of State Controller	\$ 9,815,588	\$ 206,595	2.10%
Office of State Personnel	\$ 7,360,000	\$ 13,819	0.19%
Secretary of State	\$ 8,304,184	\$ 47,103	0.57%
Wildlife Resources Commission	\$ 49,573,180	\$ 44,788	0.09%
STATEWIDE TOTAL	\$ 9,103,912,379	\$ 14,015,968	0.15%

⁵ Office of the Lt. Governor is under the umbrella of the Department of Administration.

⁶ Information Technology Services is under the umbrella of the Office of the Governor.

Statewide Security Assessment Summary Report

Version No. FV01

May 2004

Figure 7: Physical Security Expenditure as a Percentage of Operating Budgets

Agency	FY 03–04 Agency Operating Budget		FY 03–04 Physical Security Expenditure (Actual and Projected)	Physical Security Exp. as % of Agency Operating Budget
Department of Administration	\$ 145,000,000		\$ 1,323,619	0.91%
Office of the Lieutenant Governor ⁷	\$ 601,722		\$ -	0.00%
<i>Subtotal:</i>	\$ 145,601,722		\$ 1,323,619	0.91%
Department of Agriculture and Consumer Services	\$ 91,332,520		\$ 63,007	0.07%
Department of Commerce	\$ 1,069,772		\$ 21,545	2.01%
Department of Corrections	\$ 992,590,000		\$ 171,558	0.02%
Department of Crime Control and Public Safety	\$ 188,703,529		\$ 5,524	0.00%
Department of Cultural Resources	\$ 55,911,271		\$ 39,080	0.07%
Department of Environment and Natural Resources	\$ 290,355,198		\$ 1,199	0.00%
Department of Health and Human Services	\$ 3,225,850,216		\$ 890,135	0.03%
Department of Insurance	\$ 26,687,485		\$ 64,464	0.24%
Department of Justice	\$ 95,688,196		\$ 185,017	0.19%
Department of Juvenile Justice and Delinquency Prevention	\$ 132,180,585		\$ 32,038	0.02%
Department of Labor	\$ 27,019,036		\$ 25,707	0.10%
Department of Public Instruction	\$ 31,459,678		\$ 1,025	0.00%
Department of Revenue	\$ 76,200,000		\$ 669,489	0.88%
Department of State Treasurer	\$ 35,055,313		\$ 677	0.00%
Department of Transportation	\$ 3,247,069,755		\$ 1,841,587	0.06%
Employment Security Commission	\$ 161,465,750		\$ 175,450	0.11%
NC Community College System	\$ 34,442,728		\$ 450	0.00%
Office of Information Technology Services	\$ 147,652,207		\$ 242,850	0.16%
Office of the Governor ⁸	\$ 5,215,781		\$ -	0.00%
<i>Subtotal:</i>	\$ 152,867,988		\$ 242,850	0.16%
Office of State Auditor	\$ 13,096,880		\$ 111	0.00%
Office of State Budget and Management	\$ 4,211,805		\$ -	0.00%
Office of State Controller	\$ 9,815,588		\$ 31,615	0.32%
Office of State Personnel	\$ 7,360,000		\$ 9,300	0.13%
Secretary of State	\$ 8,304,184		\$ -	0.00%
Wildlife Resources Commission	\$ 49,573,180		\$ -	0.00%
STATEWIDE TOTAL	\$ 9,103,912,379		\$ 5,795,447	0.06%

⁷ Office of the Lt. Governor is under the umbrella of the Department of Administration.

⁸ Information Technology Services is under the umbrella of the Office of the Governor.

Figure 8: Business Continuity Planning Expenditure as a Percentage of Operating Budgets

Agency	FY 03–04 Agency Operating Budget	FY 03–04 Business Continuity Planning (BCP) (Actual and Projected)	BCP Exp. as % of Agency Operating Budget
Department of Administration	\$ 145,000,000	\$ -	0.00%
Office of the Lieutenant Governor ⁹	\$ 601,722	\$ 802	0.13%
<i>Subtotal:</i>	\$ 145,601,722	\$ 802	0.00%
Department of Agriculture and Consumer Services	\$ 91,332,520	\$ 22,285	0.02%
Department of Commerce	\$ 1,069,772	\$ -	0.00%
Department of Corrections	\$ 992,590,000	\$ 353,379	0.04%
Department of Crime Control and Public Safety	\$ 188,703,529	\$ 37,300	0.02%
Department of Cultural Resources	\$ 55,911,271	\$ -	0.00%
Department of Environment and Natural Resources	\$ 290,355,198	\$ 3,960	0.00%
Department of Health and Human Services	\$ 3,225,850,216	\$ 26,386	0.00%
Department of Insurance	\$ 26,687,485	\$ 35,000	0.13%
Department of Justice	\$ 95,688,196	\$ 30,342	0.03%
Department of Juvenile Justice and Delinquency Prevention	\$ 132,180,585	\$ 11,704	0.01%
Department of Labor	\$ 27,019,036	\$ 21,265	0.08%
Department of Public Instruction	\$ 31,459,678	\$ 163,726	0.52%
Department of Revenue	\$ 76,200,000	\$ 393,563	0.52%
Department of State Treasurer	\$ 35,055,313	\$ 342,381	0.98%
Department of Transportation	\$ 3,247,069,755	\$ 731,738	0.02%
Employment Security Commission	\$ 161,465,750	\$ 121,800	0.08%
NC Community College System	\$ 34,442,728	\$ -	0.00%
Office of Information Technology Services	\$ 147,652,207	\$ 2,565,314	1.74%
Office of the Governor ¹⁰	\$ 5,215,781	\$ 4,041	0.08%
<i>Subtotal:</i>	\$ 152,867,988	\$ 2,569,355	1.68%
Office of State Auditor	\$ 13,096,880	\$ 3,527	0.03%
Office of State Budget and Management	\$ 4,211,805	\$ -	0.00%
Office of State Controller	\$ 9,815,588	\$ 236,063	2.40%
Office of State Personnel	\$ 7,360,000	\$ 559	0.01%
Secretary of State	\$ 8,304,184	\$ 22,926	0.28%
Wildlife Resources Commission	\$ 49,573,180	\$ -	0.00%
STATEWIDE TOTAL	\$ 9,103,912,379	\$ 5,128,061	0.06%

⁹ Office of the Lt. Governor is under the umbrella of the Department of Administration.

¹⁰ Information Technology Services is under the umbrella of the Office of the Governor.

Statewide Security Assessment Summary Report

Version No. FV01
May 2004

Figure 9: Security and BCP Expenditures as a Percentage of Total Budget

Agency	FY 03–04 Agency Operating Budget	<u>Budget</u>	<u>Total Expenditures</u>	
		FY 03–04 Security and BCP (includes IT security, physical security and business continuity planning (BCP))	FY 03–04 Security Expenditures (Actual and Projected), includes IT security, physical, and BCP	FY 03–04 Security Expenditures (Actual and Projected) as % of Agency Operating Budget
Department of Administration	\$ 145,000,000	\$ 339,644	\$ 1,350,262	0.93%
Office of the Lieutenant Governor ¹¹	\$ 601,722	\$ 8,775	\$ 8,775	1.46%
<i>Subtotal:</i>	\$ 145,601,722	\$ 348,419	\$ 1,359,037	0.93%
Department of Agriculture and Consumer Services	\$ 91,332,520	\$ 297,936	\$ 297,936	0.33%
Department of Commerce	\$ 1,069,772	\$ 63,076	\$ 63,076	5.90%
Department of Corrections	\$ 992,590,000	\$ 948,277	\$ 948,277	0.10%
Department of Crime Control and Public Safety	\$ 188,703,529	\$ 156,107	\$ 156,107	0.08%
Department of Cultural Resources	\$ 55,911,271	\$ 43,016	\$ 43,016	0.08%
Department of Environment and Natural Resources	\$ 290,355,198	\$ 276,158	\$ 276,158	0.10%
Department of Health and Human Services	\$ 3,225,850,216	\$ 3,771,655	\$ 3,588,226	0.11%
Department of Insurance	\$ 26,687,485	\$ 248,942	\$ 248,941	0.93%
Department of Justice	\$ 95,688,196	\$ 755,834	\$ 784,126	0.82%
Department of Juvenile Justice and Delinquency Prevention	\$ 132,180,585	\$ 228,153	\$ 228,153	0.17%
Department of Labor	\$ 27,019,036	\$ 258,588	\$ 258,588	0.96%
Department of Public Instruction	\$ 31,459,678	\$ 799,458	\$ 799,458	2.54%
Department of Revenue	\$ 76,200,000	\$ 1,084,138	\$ 2,197,122	2.88%
Department of State Treasurer	\$ 35,055,313	\$ 638,017	\$ 632,816	1.81%
Department of Transportation	\$ 3,247,069,755	\$ 2,074,359	\$ 3,152,462	0.10%
Employment Security Commission	\$ 161,465,750	\$ 723,593	\$ 723,593	0.45%
NC Community College System	\$ 34,442,728	\$ 11,450	\$ 11,450	0.03%
Office of Information Technology Services	\$ 147,652,207	\$ 9,516,600	\$ 8,482,514	5.74%
Office of the Governor ¹²	\$ 5,215,781	\$ 20,304	\$ 20,124	0.39%
<i>Subtotal:</i>	\$ 152,867,988	\$ 9,536,904	\$ 8,502,638	5.56%
Office of State Auditor	\$ 13,096,880	\$ 38,069	\$ 38,069	0.29%

¹¹ Office of the Lt. Governor is under the umbrella of the Department of Administration.

¹² Information Technology Services is under the umbrella of the Office of the Governor.

Statewide Security Assessment Summary Report

Version No. FV01

May 2004

Agency	FY 03-04 Agency Operating Budget	<u>Budget</u>	<u>Total Expenditures</u>	
		FY 03-04 Security and BCP (includes IT security, physical security and business continuity planning (BCP))	FY 03-04 Security Expenditures (Actual and Projected), includes IT security, physical, and BCP	FY 03-04 Security Expenditures (Actual and Projected) as % of Agency Operating Budget
Office of State Budget and Management	\$ 4,211,805	\$ 18,000	\$ 17,463	0.41%
Office of State Controller	\$ 9,815,588	\$ 474,275	\$ 474,274	4.83%
Office of State Personnel	\$ 7,360,000	\$ 15,000	\$ 23,678	0.32%
Secretary of State	\$ 8,304,184	\$ 70,029	\$ 70,029	0.84%
Wildlife Resources Commission	\$ 49,573,180	\$ 44,788	\$ 44,788	0.09%
STATEWIDE TOTAL	\$ 9,103,912,379	\$ 22,924,240	\$ 24,939,480	0.27%

Figure 10: FY03–04 Security and Business Continuity Expenditure Detail

	D	=	A	+	B	+	C
Agency	Total Expenditures FY 03–04 Security Expenditures (Actual and Projected), includes IT security, physical, and BCP		Expenditures FY 03–04 IT Security Expenditure (Actual and Projected)		Expenditures FY 03–04 Physical Security Expenditure (Actual and Projected)		Expenditures FY 03–04 Business Continuity Planning (BCP) (Actual and Projected)
Department of Administration	\$ 1,350,262		\$ 26,643		\$ 1,323,619		\$ -
Office of the Lieutenant Governor ¹³	\$ 8,775		\$ 7,973		\$ -		\$ 802
Subtotal:	\$ 1,359,037		\$ 34,616		\$ 1,323,619		\$ 802
Department of Agriculture and Consumer Services	\$ 297,936		\$ 212,644		\$ 63,007		\$ 22,285
Department of Commerce	\$ 63,076		\$ 41,531		\$ 21,545		\$ -
Department of Corrections	\$ 948,277		\$ 423,340		\$ 171,558		\$ 353,379
Department of Crime Control and Public Safety	\$ 156,107		\$ 113,283		\$ 5,524		\$ 37,300
Department of Cultural Resources	\$ 43,016		\$ 3,936		\$ 39,080		\$ -
Department of Environment and Natural Resources	\$ 276,158		\$ 270,999		\$ 1,199		\$ 3,960
Department of Health and Human Services	\$ 3,588,226		\$ 2,671,705		\$ 890,135		\$ 26,386
Department of Insurance	\$ 248,941		\$ 149,477		\$ 64,464		\$ 35,000
Department of Justice	\$ 784,126		\$ 568,767		\$ 185,017		\$ 30,342
Department of Juvenile Justice and Delinquency Prevention	\$ 228,153		\$ 184,411		\$ 32,038		\$ 11,704
Department of Labor	\$ 258,588		\$ 211,616		\$ 25,707		\$ 21,265
Department of Public Instruction	\$ 799,458		\$ 634,706		\$ 1,025		\$ 163,726
Department of Revenue	\$ 2,197,122		\$ 1,134,069		\$ 669,489		\$ 393,563

¹³ Office of the Lt. Governor is under the umbrella of the Department of Administration.

Statewide Security Assessment Summary Report

Version No. FV01
May 2004

	D	=	A	+	B	+	C
Agency	Total Expenditures FY 03–04 Security Expenditures (Actual and Projected), includes IT security, physical, and BCP		Expenditures FY 03–04 IT Security Expenditure (Actual and Projected)		Expenditures FY 03–04 Physical Security Expenditure (Actual and Projected)		Expenditures FY 03–04 Business Continuity Planning (BCP) (Actual and Projected)
Department of State Treasurer	\$ 632,816		\$ 289,757		\$ 677		\$ 342,381
Department of Transportation	\$ 3,152,462		\$ 579,137		\$ 1,841,587		\$ 731,738
Employment Security Commission	\$ 723,593		\$ 426,343		\$ 175,450		\$ 121,800
NC Community College System	\$ 11,450		\$ 11,000		\$ 450		\$ -
Office of Information Technology Services	\$ 8,482,514		\$ 5,674,350		\$ 242,850		\$ 2,565,314
Office of the Governor ¹⁴	\$ 20,124		\$ 16,083		\$ -		\$ 4,041
<i>Subtotal:</i>	\$ 8,502,638		\$ 5,690,433		\$ 242,850		\$ 2,569,355
Office of State Auditor	\$ 38,069		\$ 34,430		\$ 111		\$ 3,527
Office of State Budget and Management	\$ 17,463		\$ 17,463		\$ -		\$ -
Office of State Controller	\$ 474,274		\$ 206,595		\$ 31,615		\$ 236,063
Office of State Personnel	\$ 23,678		\$ 13,819		\$ 9,300		\$ 559
Secretary of State	\$ 70,029		\$ 47,103		\$ -		\$ 22,926
Wildlife Resources Commission	\$ 44,788		\$ 44,788		\$ -		\$ -
STATEWIDE TOTAL	\$ 24,939,480		\$ 14,015,968		\$ 5,795,447		\$ 5,128,061

¹⁴ Information Technology Services is under the umbrella of the Office of the Governor.

Appendices

Appendix A: Agencies and Commissions included in the Assessment and Assigned Assessment Vendor.....	61
Appendix B: ISO 17799 — Synopsis	63
Appendix C: Supporting Graphics.....	66
Appendix D: Security Policy Gap Analysis Summary	70
Appendix E: Agency Security Posture	73
Appendix F: Security Remediation Estimate Detail	74
Appendix G: Distribution of Agency Security Scores	83

Appendix A: Agencies and Commissions included in the Assessment and Assigned Assessment Vendor

Project Management Office (PMO) vendor — Gartner, Inc.

(Alphabetical within Group)

Assessment Group 1	
Agency	Vendor
Department of Administration	HCS Systems, Inc.
Department of Corrections	CIBER, Inc.
Department of Environment & Natural Resources	Secure Enterprise Computing
Department of Health & Human Services	Ernst & Young, LLP
Department of Labor	Alphanumeric Systems, Inc.
Dept of Transportation	Unisys Corporation
Office of Information Technology Services (ITS)	Pomeroy IT Solutions
Office of the Secretary of State	Alphanumeric Systems, Inc.
Office of the State Auditor	Cii Associates, Inc.
Wildlife Resources Commission	Secure Enterprise Computing

Assessment Group 2	
Agency	Vendor
Community College System	Secure Enterprise Computing
Department of Agriculture	Cii Associates, Inc.
Department of Commerce	Alphanumeric Systems, Inc.
Department of Crime Control	CIBER, Inc.
Department of Insurance	Cii Associates, Inc.
Department of Juvenile Justice & Delinquency Prevention	HCS Systems, Inc.
Department of Public Instruction	Pomeroy IT Solutions

Assessment Group 3	
Agency	Vendor
Department of Cultural Resources	Cii Associates, Inc.
Department of Justice	Pomeroy IT Solutions
Department of Revenue	HCS Systems, Inc.
Department of State Treasurer	Cii Associates, Inc.
Employment Security Commission	Secure Enterprise Computing
Office of State Budget and Management	CIBER, Inc.

Statewide Security Assessment Summary Report

Version No. FV01

May 2004

Assessment Group 3	
Agency	Vendor
Office of State Controller	Unisys Corporation
Office of State Personnel	CIBER, Inc.
Office of the Governor ¹⁵	Alphanumeric Systems, Inc.
Office of the Lieutenant Governor ¹⁶	Alphanumeric Systems, Inc.

¹⁵ Information Technology Services is under the umbrella of the Office of the Governor.

¹⁶ Office of the Lt. Governor is under the umbrella of the Department of Administration.

Appendix B: ISO 17799 — Synopsis

Introduction

ISO 17799 is an internationally recognized Information Security Management Standard, first published by the International Organization for Standardization, or ISO (www.iso.ch), in December 2000. ISO 17799 is high-level, broad in scope and conceptual in nature. This approach allows it to be applied across multiple types of enterprises and applications.

ISO 17799 defines information as an asset that may exist in many forms and has value to an organization. The goal of information security is to suitably protect this asset in order to ensure business continuity, minimize business damage, and maximize return on investments. As defined by ISO 17799, information security is characterized as the preservation of:

- **Confidentiality** — ensuring that information is accessible only to those authorized to have proper authority to view the data.
- **Integrity** — safeguarding the accuracy and completeness of information and processing methods.
- **Availability** — ensuring that authorized users have access to information and associated assets when required.
- **Auditability** — ensuring that the information remains correct throughout its life.

ISO 17799 gives recommendations for information security management for use by those who are responsible for initiating, documenting, implementing or maintaining security in their organization. The standard is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in the security of inter-organizational dealings. It specifies requirements for security controls to be implemented according to the needs of individual organizations.

ISO 17799 also specifies requirements for establishing, implementing and documenting information security management systems (ISMSs). It specifies requirements for security controls to be implemented according to the needs of individual organizations.

ISO 17799 is a detailed security standard. It is organized into 10 major sections, each covering a different topic or area:

1. Business Continuity Planning

The objectives of this section are to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

2. System Access Control

The objectives of this section are: 1) to control access to information; 2) to prevent unauthorized access to information systems; 3) to ensure the protection of networked services; 4) to prevent

unauthorized computer access; 5) to detect unauthorized activities; and 6) to ensure information security when using mobile computing and tele-networking facilities.

3. System Development and Maintenance

The objectives of this section are: 1) to ensure security is built into operational systems; 2) to prevent loss, modification or misuse of user data in application systems; 3) to protect the confidentiality, authenticity and integrity of information; 4) to ensure IT projects and support activities are conducted in a secure manner; and 5) to maintain the security of application system software and data.

4. Physical and Environmental Security

The objectives of this section are: 1) to prevent unauthorized access, damage and interference to business premises and information; 2) to prevent loss, damage or compromise of assets and interruption to business activities; and 3) to prevent compromise or theft of information and information processing facilities.

5. Compliance

The objectives of this section are: 1) to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements; 2) to ensure compliance of systems with organizational security policies and standards; and 3) to maximize the effectiveness of and to minimize interference to/from the system audit process.

6. Personnel Security

The objectives of this section are: 1) to reduce risks of human error, theft, fraud or misuse of facilities; 2) to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; and 3) to minimize the damage from security incidents and malfunctions and learn from such incidents.

7. Security Organization

The objectives of this section are: 1) to manage information security within the Company; 2) to maintain the security of organizational information processing facilities and information assets accessed by third parties; and 3) to maintain the security of information when the responsibility for information processing has been outsourced to another organization.

8. Computer and Operations Management

The objectives of this section are: 1) to ensure the correct and secure operation of information processing facilities; 2) to minimize the risk of systems failures; 3) to protect the integrity of software and information; 4) to maintain the integrity and availability of information processing and communication; 5) to ensure the safeguarding of information in networks and the protection of the supporting infrastructure; 6) to prevent damage to assets and interruptions to business activities; and 7) to prevent loss, modification or misuse of information exchanged between organizations.

9. Asset Classification and Control

The objectives of this section are: 1) to maintain appropriate protection of corporate assets; and 2) to ensure that information assets receive an appropriate level of protection.

10. Security Policy

The objectives of this section are to provide management direction and support for information security.

Appendix C: Supporting Graphics

State Average Quality and Average Execution Scores by Sub-Category

Figures 11 and 12 chart the State's average Quality and average Execution scores for the 40 sub-categories encompassed in the assessment framework. In general, the figure demonstrates that the State's overall security posture scores in the "Minimal/Fair" range for most categories, with a few of the categories scoring in the "Poor" range.

Quality Score Dimension

The Quality score represents whether an agency has effectively and completely addressed its information security requirements through its Policies, Standards and Procedures (PSPs).

Quality scores mean the following:

- "Superior" indicates that the PSPs conform to best practices
- "Solid" indicates that PSPs meet requirements
- "Minimal/Fair" indicates that the PSPs are deficient
- "Poor" indicates that the PSPs do not meet requirements

Execution Score Dimension

The Execution score represents whether an agency has deployed information security Policies, Standards and Procedures in an encompassing fashion. Execution scores mean the following:

- "Superior" indicates that the PSPs are fully or universally deployed
- "Solid" indicates that the PSPs are deployed for critical areas only
- "Minimal/Fair" indicates that there are significant gaps in the deployment of PSPs
- "Poor" indicates that there are no PSPs in effect or implemented, or that PSPs are still in development

Figure 11: Average Security Quality and Execution Score by Sub-Category

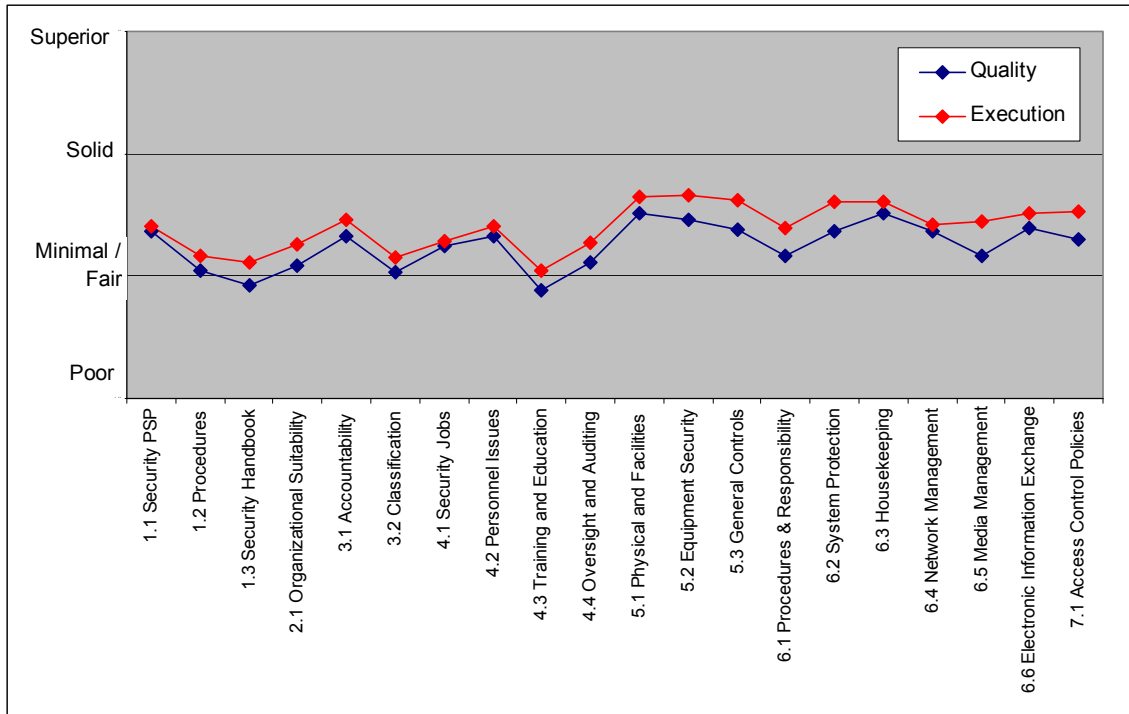


Figure 12: Average Security Quality and Execution Score by Sub-category

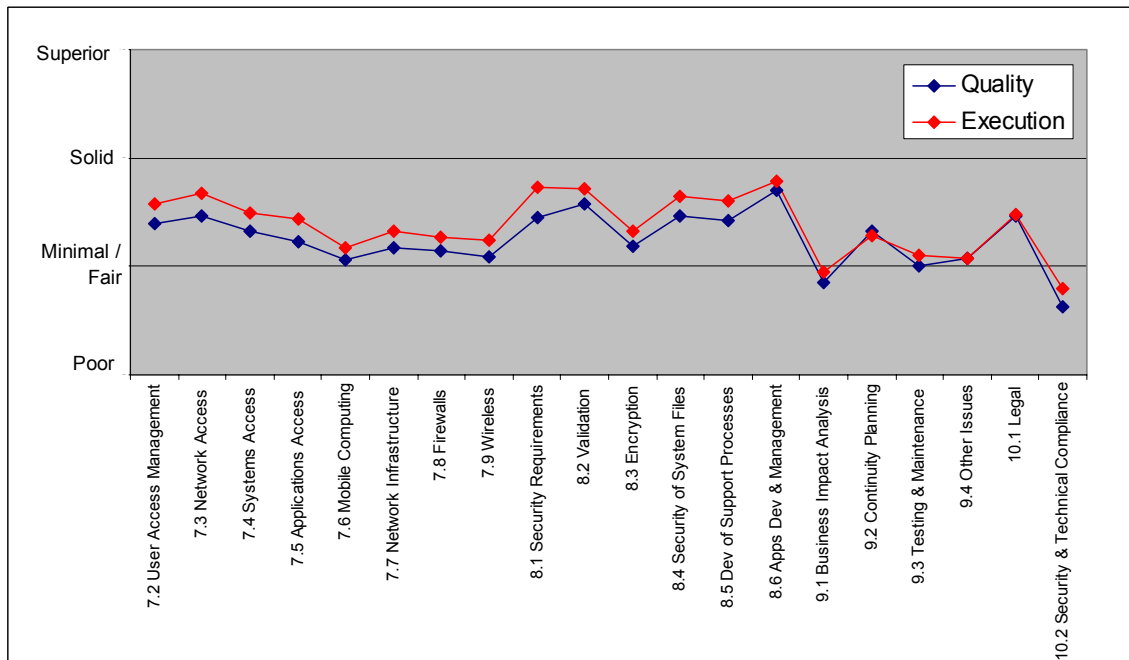


Figure 13 illustrates the State's average Quality and average Execution assessment scores for each category of the State's security policy framework. Categories that have a stronger security posture will scribe a set of points closer to the center of the graph or, in other terms, closer to the "bull's eye".

Figure 13: Average Security Quality Score vs. Average Security Execution Score (by Category)

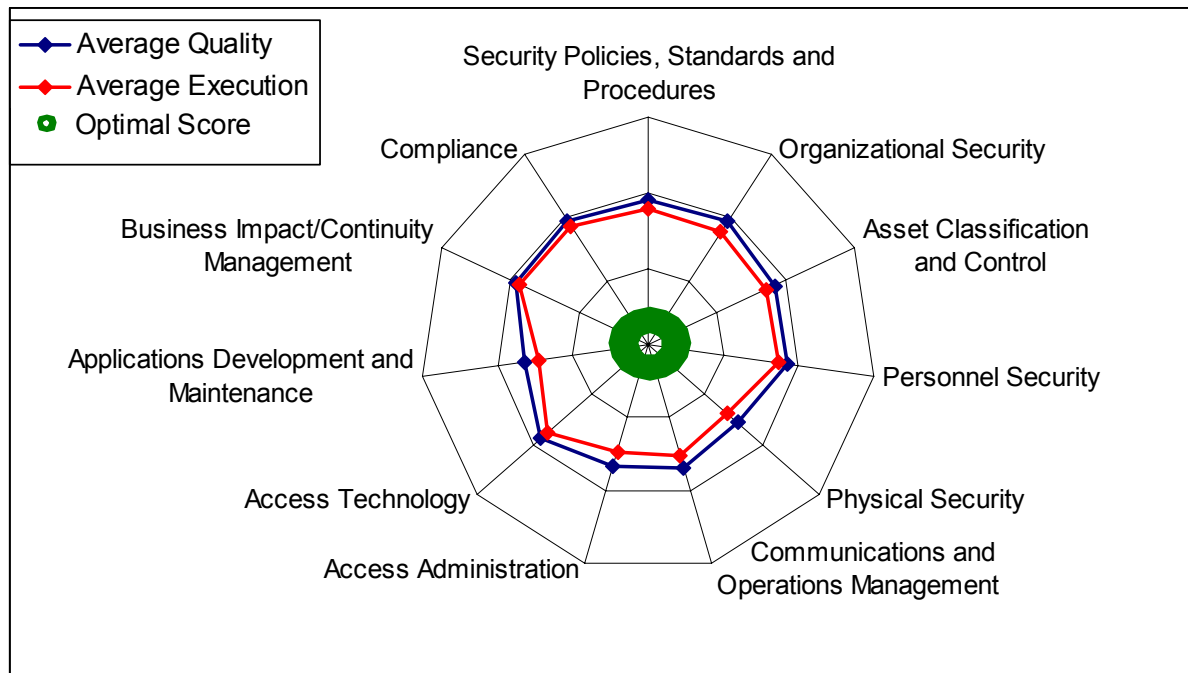


Figure 14: Average Security Scores by Agency Size

Agency Size	Average Quality	Rating	Average Execution	Rating
Large	3.15	Minimal/Fair	2.88	Minimal/Fair
Medium	2.43	Solid	2.35	Solid
Small	3.10	Minimal/Fair	2.89	Minimal/Fair

Figure 15: Average Security Scores by Project Grouping

Group	Average Quality	Rating	Average Execution	Rating
1	2.88	Minimal/Fair	2.72	Minimal/Fair
2	2.89	Minimal/Fair	2.71	Minimal/Fair
3	2.65	Minimal/Fair	2.52	Minimal/Fair

Figure 16: Sizes of Agencies by Group

Assessment Group	Large	Medium	Small	Number of Agencies in Group
Group 1	3	2	5	10
Group 2		4	3	7
Group 3 ¹⁷		5	3	8
Number of Agencies by Size	3	11	11	25

¹⁷ Excludes Office of the Governor and Office of the Lt. Governor.

Appendix D: Security Policy Gap Analysis Summary

The chart below represents a summary of the gaps in the State's security Policies, Standards and Procedures (PSPs) developed in 2003. The chart shows the indexed Policy, Standard or Procedure as well as the level of attention (i.e., Status) needed in that area. Status of each standard is defined as:

- ❑ **Severe:** if no supporting materials exist that adequately address the PSPs
- ❑ **Moderate:** if no supporting materials exist that adequately address the PSPs, but does not represent a widespread problem area
- ❑ **Low:** if supporting materials exist that adequately address the PSPs

Policy, Standard or Procedure	Status
100 Information Security Program Charter	
110 Information Security Policies, Standards and Procedures	MODERATE
110-01 Publishing Policies, Standards and Procedures	MODERATE
110-01-01 Process for Publishing Policies, Standards and Procedures	MODERATE
110-01-02 Tracking and Reporting Non-compliance with Policies	MODERATE
120 Information Security Infrastructure	
120-01 Assignment of Information Security Roles and Responsibilities	MODERATE
121 Information Security Program	SEVERE
121-01 Information Security Metrics and Communication Standard	MODERATE
122 Security of Third-Party Access	MODERATE
122-01 Third-Party Access Security Standard	LOW
122-01-01 Third-Party Access Request Procedure	LOW
123 Outsourcing and Contracting	MODERATE
123-01 Outsourcing and Contracting Requirements Standard	LOW
130 Enterprise Systems Architecture	SEVERE
130-01 Enterprise Security Architecture Documentation Standard	LOW
131 Inventory and Classification of Information Assets	SEVERE
131-01 Information Asset Inventory and Classification Standard	MODERATE
131-01-01 Performing a Risk Assessment	SEVERE
132 Privacy of Personal Information	LOW
132-01 Standard for Collecting Personally Identifiable Information	MODERATE
132-02 Web Site Privacy Policy Standard	MODERATE
140 Security in Job Definition and Resourcing	MODERATE
140-01 Employee Security and Non-disclosure Agreements	MODERATE
141 Information Security Education and Training	MODERATE
141-01 Security Awareness Training Standard	MODERATE
141-02 Specialized Security Training Standard	LOW
142 Responding to Security Incidents and Malfunctions	MODERATE
142-00-01 Reporting Incidents	MODERATE
150 Secure Areas	LOW
150-01 Secure Facilities Standard	LOW
150-01-01 Obtaining Access to Secure ITS Facilities	LOW

Statewide Security Assessment Summary Report

Version No. FV01
May 2004

Policy, Standard or Procedure	Status
151 Equipment Security	LOW
151-01 Secure Disposal or Reuse of Equipment	LOW
151-01-01 Documenting Disposal or Release of Previously Classified Equipment	LOW
152 General Controls	LOW
152-01 Maintenance and Removal of Equipment	LOW
160 Operational Procedures and Responsibilities	LOW
160-01 Standards for Separation of Duties	LOW
161 Incident Management	SEVERE
161-00-01 Incident Response Process	SEVERE
162 Protection Against Malicious Software	LOW
162-01 Virus Protection	MODERATE
162-01-01 Updating Virus Signatures (Agency Only)	
162-02 Approved Software Download List (Agency Only)	
162-02-01 Process for Requesting Approval to Install Software (Agency Only)	
163 Housekeeping	LOW
163-01 System Backup and Off-Site Storage	LOW
163-01-01 System Backup and Off-Site Storage Procedure	LOW
163-02 Operator Logs and Fault Logging	LOW
163-02-01 Restoration of Systems from Backups	LOW
164 Media Handling and Security	MODERATE
164-01 Standards for Clearing or Destroying Media	LOW
165 Exchanges of Information and Software	MODERATE
165-01 Protecting Electronic Communications	MODERATE
165-02 MS Exchange Secure Configuration	MODERATE
170 Business Requirement for Access Control	LOW
171 User Access Management	LOW
171-00-01 Using ITS Directory Services	LOW
171-01 UserID and Password Protection	
171-02 Privileged Users Standard	MODERATE
171-02-01 Authorization Process for Obtaining System Privileges	LOW
172 User Responsibilities	LOW
172-00-01 Approval Process for Use of Personal Equipment or Software (Agency Only)	
173 Network Access Control	LOW
173-01 DNS Enterprise Security Standard	
173-02 IEEE 802.11 Wireless Network Access Security Standard	
173-03 Firewall Configuration Security Standard	SEVERE
173-04 Router Configuration Security Standard	SEVERE
173-05 VPN Standard	MODERATE
173-06 Modem Standard	SEVERE
174 Operating System and Database Access Control	SEVERE

Statewide Security Assessment Summary Report

Version No. FV01

May 2004

Policy, Standard or Procedure	Status
174-01 Windows 2000 Security Standard	MODERATE
174-02 UNIX Security Standard	MODERATE
174-03 RACF Security Standard	LOW
174-04 IIS Security Standard	SEVERE
174-05 Oracle Security Standard	MODERATE
174-06 SQL Server Security Standard	MODERATE
174-07 Desktop Security Standard	LOW
175 Application Access Control	MODERATE
176 Monitoring System Access and Use	MODERATE
176-01 Monitoring and Auditing	MODERATE
177 Mobile Computing and Telecommuting	SEVERE
177-01 Remote Access Security Standard	
177-02 Laptop Security Standard	MODERATE
177-03 Protection for Mobile Devices	MODERATE
177-04 Standards for Telecommuting	MODERATE
180 Life Cycle Change Management	SEVERE
180-00-01 Change Management and Systems Acceptance Process	SEVERE
181 Security in Application Systems	
181-01 Standards for Secure Application Development	SEVERE
182 Cryptographic Controls	LOW
182-01 Standards for PKI and other Cryptographic Technologies	MODERATE
183 Vulnerability Management	SEVERE
183-01 Vulnerability Management Standard	
184 Threat Assessment and Monitoring	MODERATE
184-00-01 Collection and Dissemination of Threat Warnings	MODERATE
184-01 Intrusion Detection	MODERATE
190 Aspects of Business Continuity Management	LOW
190-00-01 Disaster Recovery Plan	LOW
190-00-02 Business Continuity Plan	LOW
200 Compliance with Legal Requirements	MODERATE
200-01 Notifications and Warning Banners	LOW
201 Reviews of Security Policy and Technical Compliance	MODERATE
201-01 Security Requirements Matrix	LOW
201-02 Vulnerability Assessment Standard	MODERATE
201-02-01 Performing Compliance Reviews	MODERATE
202 System Audit Considerations	MODERATE
202-01 Standard for Protection of Compliance Tools and Output	MODERATE

Appendix E: Agency Security Posture

The chart below shows the agency posture averaging to the two dimensions assessed: Quality and Execution.

Figure 17: Translation of Security Assessment Scores

Assessment Score	Posture
1.00 to 1.19	Superior
1.20 to 1.39	Superior
1.40 to 1.59	Superior
1.60 to 1.78	Solid
1.80 to 1.99	Solid
2.00 to 2.19	Solid
2.20 to 2.39	Solid
2.40 to 2.59	Minimal/Fair
2.60 to 2.79	Minimal/Fair
2.80 to 2.99	Minimal/Fair
3.00 to 3.19	Minimal/Fair
3.20 to 3.39	Poor
3.40 to 4.00	Poor

Appendix F: Security Remediation Estimate Detail

Figure 18: Cost Estimates by Security Finding — Expense/Capital Breakout

Finding	Recommendation	Enterprise			Agency		
		Initial Expense Outlay	Initial Capital Outlay	Ongoing Operating Costs	Initial Expense Outlay	Initial Capital Outlay	Ongoing Operating Costs
Insufficient Funding	E1: Increase Funding to Enhance Enterprise Program Office	526,400	1,500,000	1,821,360			
	A1: Increase Funding to Agencies						15,196,640
Deficient and Absent Policies, Standards, and Procedures	E2: Complete Statewide Security Framework	387,200		35,000			
	A2: Improve Agency Security Policies, Standards, and Procedures				1,542,800		364,000
Insufficient Levels of Staffing	A3: Increase Level of Security Staffing				2,144,800		2,144,800
Security Experience is Lacking	E3: Improve Enterprise Security Awareness and Training	304,000	200,000	205,600			
	A4: Improve Agency Security Awareness and Training				431,200		436,800
Outdated Desktop Operating Systems	A5: Replace Outdated Desktop Operating Systems					38,820,000	
Gaps in Agency Border / Perimeter Defense	A6: Improve Agency Border / Perimeter Defense				152,880	1,392,000	374,800
Outdated and Incomplete Risk and Business Continuity Management	E4: Improve Risk Management and Business Continuity Plans	2,032,800		1,307,990			
	A7: Improve Risk Management and Business Continuity Plans				3,466,800		11,771,910
	Totals:	3,250,400	1,700,000	3,369,950	7,738,480	40,212,000	30,288,950

Figure 19: Cost Estimates by Security Finding — Expense/Capital Summary

Finding	Recommendation	Total		
		Total Initial Expense	Total Initial Capital	Total Ongoing Operating Costs
Insufficient Funding	E1: Increase Funding to Enhance Enterprise Program Office	526,400	1,500,000	1,821,360
	A1: Increase Funding to Agencies			15,196,640
		526,400	1,500,000	17,018,000
Deficient and Absent Policies, Standards, and Procedures	E2: Complete Statewide Security Framework	387,200		35,000
	A2: Improve Agency Security Policies, Standards, and Procedures	1,542,800		364,000
		1,930,000		399,000
Insufficient Levels of Staffing	A3: Increase Level of Security Staffing	2,144,800		2,144,800
Security Experience is Lacking	E3: Improve Enterprise Security Awareness and Training	304,000	200,000	205,600
	A4: Improve Agency Security Awareness and Training	431,200		436,800
		735,200	200,000	642,400
Outdated Desktop Operating Systems	A5: Replace Outdated Desktop Operating Systems		38,820,000	
Gaps in Agency Border / Perimeter Defense	A6: Improve Agency Border / Perimeter Defense	152,880	1,392,000	374,800
Outdated and Incomplete Risk and Business Continuity Management	E4: Improve Risk Management and Business Continuity Plans	2,032,800		1,307,990
	A7: Improve Risk Management and Business Continuity Plans	3,466,800		11,771,910
Totals:		10,988,880	41,912,000	33,658,900

Figure 20: Workday Estimates for Enterprise-Level Security Recommendations

Recommendation	Internal Workdays Estimate	External Workdays Estimate
E1: Increase Funding to Enhance Enterprise Program Office		
Three Month Planning Effort - Enterprise Program	120	60
Enterprise Security Program Improvement Implementations	220	220
E2: Complete Statewide Security Framework		
Complete Policies from the GAP analysis	220	220
E3: Improve Enterprise Security Awareness and Training		
Develop Training Materials	120	120
Develop Enterprise Level Awareness Program	80	40
E4: Improve Risk Management and Business Continuity Plans		
Conduct BIA / Risk Analysis	440	330
Create BCP / DR Planning Templates	60	60
Develop Agency Specific BCP / DR Plan	440	440
Implement Recovery Solutions	440	220

Figure 21: Cost Estimates for Enterprise-Level Security Recommendations

Recommendation	Enterprise			
	Initial Expense Outlay	Initial Capital Outlay	Total Initial Outlay	Ongoing Operating Costs
E1: Increase Funding to Enhance Enterprise Program Office	526,400	1,500,000	2,026,400	1,821,360
Three Month Planning Effort - Enterprise Program	139,200		139,200	246,400
Enterprise Security Program Improvement Implementations	387,200	1,500,000	1,887,200	1,574,960
E2: Complete Statewide Security Framework	387,200		387,200	35,000
Complete Policies from the GAP analysis	387,200		387,200	35,000
E3: Improve Enterprise Security Awareness and Training	304,000	200,000	504,000	205,600
Develop Training Materials	211,200		211,200	5,600
Develop Enterprise Level Awareness Program	92,800	200,000	292,800	200,000
E4: Improve Risk Management and Business Continuity Plans	2,032,800		2,032,800	1,307,990
Conduct BIA / Risk Analysis	642,400		642,400	
Create BCP / DR Planning Templates	105,600		105,600	
Develop Agency Specific BCP / DR Plan	774,400		774,400	
Implement Recovery Solutions	510,400		510,400	1,307,990
Totals:	3,250,400	1,700,000	4,950,400	3,369,950

Figure 22: Ongoing Operating Cost Assumptions for Enterprise-Level Security Recommendation

Recommendation	Ongoing Operating Costs	Ongoing Operating Cost Assumptions
E1: Increase Funding to Enhance Enterprise Program Office	1,821,360	Additional Two Internal Resources to Manage the Program 10% of the total incremental security expenditure
Three Month Planning Effort - Enterprise Program	246,400	
Enterprise Security Program Improvement Implementations	1,574,960	
E2: Complete Statewide Security Framework	35,000	10 Days for one person to maintain 20 days per year plus expenses for materials
Complete Policies from the GAP analysis	35,000	
E3: Improve Enterprise Security Awareness and Training	205,600	
Develop Training Materials	5,600	10% of the amount earmarked for the Business Continuity
Develop Enterprise Level Awareness Program	200,000	
E4: Improve Risk Management and Business Continuity Plans	1,307,990	
Conduct BIA / Risk Analysis	1,307,990	
Create BCP / DR Planning Templates		
Develop Agency Specific BCP / DR Plan		
Implement Recovery Solutions		
Totals:	3,369,950	

Figure 23: Workday Estimates for Agency-Level Security Recommendations

Recommendation	Small		Medium		Large		Requirements		
	Internal Workdays Estimate	External Workdays Estimate	Internal Workdays Estimate	External Workdays Estimate	Internal Workdays Estimate	External Workdays Estimate	Number of Small Agencies	Number of Medium Agencies	Number of Large Agencies
A1: Increase Funding to Agencies									
A2: Improve Agency Security Policies, Standards, and Procedures									
Tailor Policies to the Agencies	20	5	40	10	40	40	9	4	3
Develop Agency Specific Procedures	40	10	60	20	40	120	9	4	3
A3: Increase Level of Security Staffing	75		220		440		10	8	3
A4: Improve Agency Security Awareness and Training									
Tailor Training to Agencies	10		15		15		11	11	3
Conduct End User Train-the-Trainer	5		10		10		11	11	3
Conduct Security Professional Training	5		10		30		11	11	3
A5: Replace Outdated Desktop Operating Systems									
A6: Improve Agency Border / Perimeter Defense									
Improve Firewalls	5		10		20		10	6	2
Remove Modems	5		10				1	2	
Improve Wireless (Monitoring for rogue wireless hubs)	2		5		15		9	10	2
A7: Improve Risk Management and Business Continuity Plans									
Conduct BIA / Risk Analysis	10	15	20	35	40	90	11	5	3
Develop Agency Specific BCP / DR Plan	20	10	20	35	60	120	11	5	3
Implement Recovery Solutions	20	20	60	60	110	110	11	5	3

Figure 24: Cost Estimates for Agency-Level Security Recommendations

Recommendation	Initial Expense Outlay	Initial Capital Outlay	Total Initial Outlay	Ongoing Operating Costs
A1: Increase Funding to Agencies				15,196,640
A2: Improve Agency Security Policies, Standards, and Procedures	1,542,800		1,542,800	364,000
Tailor Policies to the Agencies	503,600		503,600	72,800
Develop Agency Specific Procedures	1,039,200		1,039,200	291,200
A3: Increase Level of Security Staffing	2,144,800		2,144,800	2,144,800
A4: Improve Agency Security Awareness and Training	431,200		431,200	436,800
Tailor Training to Agencies	179,200		179,200	72,800
Conduct End User Train-the-Trainer	109,200		109,200	72,800
Conduct Security Professional Training	142,800		142,800	291,200
A5: Replace Outdated Desktop Operating Systems		38,820,000	38,820,000	
A6: Improve Agency Border / Perimeter Defense	152,880	1,392,000	1,544,880	374,800
Improve Firewalls	84,000	1,370,000	1,454,000	274,000
Remove Modems	14,000		14,000	
Improve Wireless (Monitoring for rogue wireless hubs)	54,880	22,000	76,880	100,800
A7: Improve Risk Management and Business Continuity Plans	3,466,800		3,466,800	11,771,910
Conduct BIA / Risk Analysis	916,800		916,800	145,600
Develop Agency Specific BCP / DR Plan	1,054,000		1,054,000	341,600
Implement Recovery Solutions	1,496,000		1,496,000	11,284,710
Totals:	7,738,480	40,212,000	47,950,480	30,288,950

Figure 25: Ongoing Operating Cost Assumptions for Agency-Level Security Recommendations

Recommendation	Ongoing Operating Costs	Ongoing Operating Cost Assumptions
A1: Increase Funding to Agencies	15,196,640	
A2: Improve Agency Security Policies, Standards, and Procedures Tailor Policies to the Agencies Develop Agency Specific Procedures	364,000 72,800 291,200	5 days average per agency 20 days average per agency
A3: Increase Level of Security Staffing	2,144,800	
A4: Improve Agency Security Awareness and Training Tailor Training to Agencies Conduct End User Train-the-Trainer Conduct Security Professional Training	436,800 72,800 72,800 291,200	5 Days per Agency to maintain 5 Days per Agency to keep current 10 Days per year, average of 2 per agency
A5: Replace Outdated Desktop Operating Systems		
A6: Improve Agency Border / Perimeter Defense Improve Firewalls Remove Modems Improve Wireless (Monitoring for rogue wireless hubs)	374,800 274,000 100,800	Maintenance @ 20% of Hardware costs Average of 6 Days per agency to monitor
A7: Improve Risk Management and Business Continuity Plans Conduct BIA / Risk Analysis Develop Agency Specific BCP / DR Plan Implement Recovery Solutions	11,771,910 145,600 341,600 11,284,710	10 Days per Agency to maintain 15 Days per Agency to maintain 90% of the amount earmarked for the Business Continuity
Totals:	30,288,950	

Recommendation 1: Calculations	
Total Statewide Spending Target	34,595,000
Current Agency Spending	14,016,000
Increase in Spending Necessary to Achieve Target Levels	20,579,000
Sum of the Ongoing Costs Identified in Recommendations 2–7	5,382,360
Additional Funding to Be Distributed to Agencies Based on Assessed Security Posture	15,196,640

Recommendation 6: Firewall Calculations					
		Acquisition and Install	Annual Maintenance @ 20%	Total Acquisition	Annual Maintenance
Large Agency					
Number of Additional Firewalls (1)					
4	Large Firewalls	\$ 50,000	\$ 10,000	\$ 200,000	\$ 40,000
25	Small Firewalls	\$ 30,000	\$ 6,000	\$ 750,000	\$ 150,000
Medium Agency					
Number of Additional Firewalls					
2	Large Firewalls	\$ 50,000	\$ 10,000	\$ 100,000	\$ 20,000
8	Small Firewalls	\$ 30,000	\$ 6,000	\$ 240,000	\$ 48,000
Small Agency					
Number of Additional Firewalls					
1	Large Firewalls	\$ 50,000	\$ 10,000	\$ 50,000	\$ 10,000
1	Small Firewalls	\$ 30,000	\$ 6,000	\$ 30,000	\$ 6,000
Totals				\$ 1,370,000	\$ 274,000

Note: (1) Gartner's estimate for the number of firewalls per agency size is based on Gartner's experience conducting similar assessments for similar sized organizations.

Appendix G: Distribution of Agency Security Scores

Included in the following pages are the 237 questions of the assessment template, the number of agencies that had a score for that question, and the distribution of scores and the percentage that that distribution represents. The scoring scale for the assessment is included below.

Quality	Execution
1=Best Practice 2=Meets Reqs 3=Deficient 4=Does Not Meet Reqs Blank = Not Applicable	1=Fully 2=Critical Areas 3=Minimal/Gaps 4=None/WIP Blank = Not Applicable

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
1.1.1 Is there an agency security PSP in place?	25	1 4.0%	8 32.0%	13 52.0%	3 12.0%	1 4.0%	9 36.0%	13 52.0%	2 8.0%
1.1.2 Does the PSP state what is and is not permissible?	25	2 8.0%	13 52.0%	8 32.0%	2 8.0%	3 12.0%	11 44.0%	9 36.0%	2 8.0%
1.1.3 Is the agency PSP in compliance with State Security PSPs?	25		15 60.0%	8 32.0%	2 8.0%		15 60.0%	8 32.0%	2 8.0%
1.1.4 Have the State PSPs been augmented to reflect unique agency requirements?	25		14 56.0%	6 24.0%	5 20.0%		13 52.0%	10 40.0%	2 8.0%
1.1.5 Does the scope of the PSP cover all facets of information?	25	2 8.0%	6 24.0%	11 44.0%	6 24.0%	3 12.0%	8 32.0%	10 40.0%	4 16.0%
1.1.6 Does the PSP define and identify what is classed as information?	25	1 4.0%	8 32.0%	6 24.0%	10 40.0%		10 40.0%	7 28.0%	8 32.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
1.1.7 Does the PSP define and identify organizational perimeters?	25		10 40.0%	5 20.0%	10 40.0%		11 44.0%	7 28.0%	7 28.0%
1.1.8 Does the PSP identify management and employee responsibilities?	25	2 8.0%	10 40.0%	7 28.0%	6 24.0%	1 4.0%	11 44.0%	10 40.0%	3 12.0%
1.1.9 Does the PSP make clear the consequences of noncompliance?	25	7 28.0%	8 32.0%	7 28.0%	3 12.0%	5 20.0%	10 40.0%	6 24.0%	4 16.0%
1.1.10 Has it been updated/reviewed in the past 12 months?	25	2 8.0%	10 40.0%	7 28.0%	6 24.0%	2 8.0%	11 44.0%	6 24.0%	6 24.0%
1.1.11 Has management approved the PSP?	25	3 12.0%	12 48.0%	7 28.0%	3 12.0%	4 16.0%	9 36.0%	9 36.0%	3 12.0%
1.1.12 Is there an information security PSP that covers contractors?	25	2 8.0%	11 44.0%	5 20.0%	7 28.0%	1 4.0%	13 52.0%	4 16.0%	7 28.0%

Distribution of Quality and Execution Scores by Question

Question		# Respon	Quality Scores				Execution Scores			
			Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
1.1.13	Does the security PSP assign responsibility and do the job descriptions reflect this responsibility?	25	1 4.0%	7 28.0%	9 36.0%	8 32.0%	1 4.0%	5 20.0%	12 48.0%	7 28.0%
1.2.1	Are procedures in place to implement the information security policy?	25	2 8.0%	8 32.0%	8 32.0%	7 28.0%	2 8.0%	8 32.0%	11 44.0%	4 16.0%
1.2.2	Are standards in place to evergreen the policies and procedures?	25	2 8.0%	4 16.0%	9 36.0%	10 40.0%	3 12.0%	4 16.0%	11 44.0%	7 28.0%
1.2.3	Does the project management methodology uphold the security practices?	25		9 36.0%	4 16.0%	12 48.0%		8 32.0%	10 40.0%	7 28.0%
1.3.1	Is there an information security employee handbook in place?	25	2 8.0%	5 20.0%	8 32.0%	10 40.0%	2 8.0%	5 20.0%	11 44.0%	7 28.0%
1.3.2	Does the handbook address the employees responsibilities?	22	1 4.5%	5 22.7%	8 36.4%	8 36.4%	2 9.1%	5 22.7%	9 40.9%	6 27.3%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
1.3.3 Does the handbook make clear the consequences of non-compliance?	22	2 9.1%	6 27.3%	3 13.6%	11 50.0%	4 18.2%	6 27.3%	3 13.6%	9 40.9%
2.1.1 Does Senior Management support (e.g., are they briefed, are metrics established, do they participate in reviews, security oversight committee, etc.) the information security program?	25	2 8.0%	5 20.0%	14 56.0%	4 16.0%	2 8.0%	8 32.0%	12 48.0%	3 12.0%
2.1.2 Is periodic reporting on the level of information security compliance (including metrics, demonstration of key requirements, compliance, etc.) issued and reviewed by management?	25	3 12.0%	3 12.0%	10 40.0%	9 36.0%	2 8.0%	6 24.0%	14 56.0%	3 12.0%
2.1.3 Are employees able to perform their duties efficiently and effectively while following security procedures?	25	1 4.0%	12 48.0%	9 36.0%	3 12.0%		17 68.0%	5 20.0%	3 12.0%
2.1.4 Does the information security program have its own line item in the budget?	25	1 4.0%		4 16.0%	20 80.0%	1 4.0%	1 4.0%	9 36.0%	14 56.0%
2.1.5 Are there any open security positions and is funding in place to meet the Agency's stated requirements?	25		7 28.0%	9 36.0%	9 36.0%	1 4.0%	6 24.0%	9 36.0%	9 36.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
2.1.6 Is there a process to submit needed security policy changes at the Agency?	25	2 8.0%	6 24.0%	9 36.0%	8 32.0%	2 8.0%	8 32.0%	13 52.0%	2 8.0%
2.1.7 Are there named security owners?	25	3 12.0%	9 36.0%	10 40.0%	3 12.0%	4 16.0%	9 36.0%	10 40.0%	2 8.0%
3.1.1 Is logical access to assets fully controlled?	25	2 8.0%	12 48.0%	9 36.0%	2 8.0%	2 8.0%	11 44.0%	10 40.0%	2 8.0%
3.1.2 Is the asset inventory complete (dB, software, hardware, services)?	25	1 4.0%	14 56.0%	9 36.0%	1 4.0%	1 4.0%	15 60.0%	9 36.0%	
3.1.3 Is there an audit log to identify the individual and the time of access for nonstandard hours of access?	25		8 32.0%	14 56.0%	3 12.0%		8 32.0%	14 56.0%	3 12.0%
3.1.4 Are procedures in place for the proper disposal of confidential information?	25	1 4.0%	5 20.0%	11 44.0%	8 32.0%	1 4.0%	11 44.0%	12 48.0%	1 4.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqmn't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
3.2.1 Is there a reasonable, complete and usable information classification policy?	25	1 4.0%	8 32.0%	8 32.0%	8 32.0%	2 8.0%	8 32.0%	9 36.0%	6 24.0%
3.2.2 Does the information classification policy fully address all relevant information?	23	1 4.3%	8 34.8%	5 21.7%	9 39.1%	2 8.7%	5 21.7%	10 43.5%	6 26.1%
3.2.3 Is the information classification policy followed?	22		8 36.4%	5 22.7%	9 40.9%	1 4.5%	8 36.4%	8 36.4%	5 22.7%
3.2.4 Is an information classification methodology in place to assist employees in identifying levels of information within the business unit?	23		6 26.1%	8 34.8%	9 39.1%		7 30.4%	11 47.8%	5 21.7%
3.2.5 Is there procedure for labeling assets and are they consistently labeled?	25	1 4.0%	15 60.0%	3 12.0%	6 24.0%	2 8.0%	13 52.0%	7 28.0%	3 12.0%
3.2.6 Is there an information handling matrix that explains how specific information resources are to be handled?	25	2 8.0%	2 8.0%	7 28.0%	14 56.0%	1 4.0%	4 16.0%	10 40.0%	10 40.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
4.1.1 Security roles and responsibilities are defined (as illustrated in the security policy)	25	2 8.0%	5 20.0%	9 36.0%	9 36.0%	1 4.0%	9 36.0%	11 44.0%	4 16.0%
4.1.2 Security is included in job descriptions across the organization?	25	2 8.0%	4 16.0%	12 48.0%	7 28.0%		6 24.0%	12 48.0%	7 28.0%
4.1.3 Personnel are screened for security on change in employment status?	24	3 12.5%	10 41.7%	6 25.0%	5 20.8%	2 8.3%	11 45.8%	6 25.0%	5 20.8%
4.1.4 Are contractors and temporary staff security screened?	25	3 12.0%	10 40.0%	5 20.0%	7 28.0%	2 8.0%	12 48.0%	4 16.0%	7 28.0%
4.1.5 Is the disciplinary process defined for security incidents?	25	3 12.0%	9 36.0%	8 32.0%	5 20.0%	2 8.0%	13 52.0%	7 28.0%	3 12.0%
4.2.1 Does the enterprise have enough employees to support current security goals?	25		6 24.0%	13 52.0%	6 24.0%		4 16.0%	16 64.0%	5 20.0%

Distribution of Quality and Execution Scores by Question

Question		Quality Scores					Execution Scores			
		# Respon	Best Practice	Meets Reqmn't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
4.2.2	Are employees and project managers aware of their responsibilities for protecting information resources?	25	1	11	7	6	1	14	9	1
			4.0%	44.0%	28.0%	24.0%	4.0%	56.0%	36.0%	4.0%
4.2.3	Are employees subject to confidentiality agreements?	25	9	8	2	6	12	6	2	5
			36.0%	32.0%	8.0%	24.0%	48.0%	24.0%	8.0%	20.0%
4.2.4	Are employees properly trained to perform security tasks?	25	1	6	9	9	1	6	12	6
			4.0%	24.0%	36.0%	36.0%	4.0%	24.0%	48.0%	24.0%
4.2.5	Does the enterprise have sufficient expertise to implement an information security awareness program?	25	4	7	8	6	3	6	11	5
			16.0%	28.0%	32.0%	24.0%	12.0%	24.0%	44.0%	20.0%
4.2.6	Are contractor personnel subject to confidentiality agreements?	25	7	10	2	6	7	10	3	5
			28.0%	40.0%	8.0%	24.0%	28.0%	40.0%	12.0%	20.0%
4.2.7	Are contract personnel specifically addressed in security PSP?	24	5	5	6	8	4	7	7	6
			20.8%	20.8%	25.0%	33.3%	16.7%	29.2%	29.2%	25.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
4.2.8 Is access to confidential information by employees and contract personnel monitored?	25		7 28.0%	11 44.0%	7 28.0%		7 28.0%	14 56.0%	4 16.0%
4.3.1 Do employees receive security-related training specific to their responsibilities (e.g., new hire, position change, etc.)?	25		7 28.0%	9 36.0%	9 36.0%	1 4.0%	5 20.0%	11 44.0%	8 32.0%
4.3.2 Are employees receiving feedback related to security on their performance evaluations?	25		6 24.0%	8 32.0%	11 44.0%	1 4.0%	6 24.0%	11 44.0%	7 28.0%
4.3.3 Is security-related training provided periodically to reflect changes and new methods?	25		6 24.0%	7 28.0%	12 48.0%	1 4.0%	7 28.0%	10 40.0%	7 28.0%
4.3.4 Are system administrators given additional security training specific to their jobs?	25	1 4.0%	6 24.0%	7 28.0%	11 44.0%	2 8.0%	5 20.0%	9 36.0%	9 36.0%
4.3.5 Are employees briefed on their responsibility to protect the property (physical and logical) of the State when working away from the Agency environment?	25	1 4.0%	9 36.0%	10 40.0%	5 20.0%	1 4.0%	11 44.0%	8 32.0%	5 20.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
4.3.6 Is there a regular security awareness and training program in place?	25		5 20.0%	5 20.0%	15 60.0%		4 16.0%	11 44.0%	10 40.0%
4.4.1 Are the security policies and procedures routinely tested?	25	1 4.0%	4 16.0%	6 24.0%	14 56.0%		5 20.0%	11 44.0%	9 36.0%
4.4.2 Are deviations to security policies and procedures documented and escalated?	25	2 8.0%	9 36.0%	6 24.0%	8 32.0%		14 56.0%	6 24.0%	5 20.0%
4.4.3 Are audit logs or other reporting mechanisms in place on all platforms, and are they reviewed?	25		6 24.0%	12 48.0%	7 28.0%		8 32.0%	15 60.0%	2 8.0%
4.4.4 When an employee is found to be in noncompliance with the security policies, has appropriate disciplinary action been taken?	25	5 20.0%	11 44.0%	4 16.0%	5 20.0%	3 12.0%	14 56.0%	5 20.0%	3 12.0%
4.4.5 Are audits performed on a regular basis?	25	1 4.0%	5 20.0%	8 32.0%	11 44.0%	3 12.0%	5 20.0%	8 32.0%	9 36.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
4.4.6 Are unscheduled audits performed?	24	1 4.2%	5 20.8%	8 33.3%	10 41.7%	1 4.2%	5 20.8%	12 50.0%	6 25.0%
4.4.7 Are security incidents tracked and remediated?	25	2 8.0%	7 28.0%	9 36.0%	7 28.0%	1 4.0%	11 44.0%	9 36.0%	4 16.0%
4.4.8 Has someone been identified as responsible for reconciling incidents and audits?	25	3 12.0%	10 40.0%	9 36.0%	3 12.0%	3 12.0%	11 44.0%	9 36.0%	2 8.0%
5.1.1 Is there a defined physical security perimeter?	25		12 48.0%	11 44.0%	2 8.0%	1 4.0%	14 56.0%	9 36.0%	1 4.0%
5.1.2 Is access to buildings controlled?	25	1 4.0%	12 48.0%	10 40.0%	2 8.0%	1 4.0%	11 44.0%	12 48.0%	1 4.0%
5.1.3 Is access to computing facilities controlled?	25	3 12.0%	17 68.0%	3 12.0%	2 8.0%	5 20.0%	13 52.0%	6 24.0%	1 4.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
5.1.4 Is there an additional level of control for after-hours access?	25	1 4.0%	17 68.0%	5 20.0%	2 8.0%	3 12.0%	16 64.0%	6 24.0%	
5.1.5 Is there an audit log to identify the individual and the time of access for nonstandard hours of access?	25	2 8.0%	15 60.0%	5 20.0%	3 12.0%	3 12.0%	12 48.0%	7 28.0%	3 12.0%
5.1.6 Are systems and other hardware adequately protected from theft?	25	2 8.0%	15 60.0%	4 16.0%	4 16.0%	2 8.0%	15 60.0%	7 28.0%	1 4.0%
5.1.7 Is there a specific policy for the control and configuration of portable equipment?	25	1 4.0%	8 32.0%	8 32.0%	8 32.0%		12 48.0%	7 28.0%	6 24.0%
5.1.8 Are physical security practices appropriate to the function?	25	3 12.0%	12 48.0%	7 28.0%	3 12.0%	2 8.0%	15 60.0%	8 32.0%	
5.1.9 Are physical security mechanisms tested?	25		9 36.0%	10 40.0%	6 24.0%	1 4.0%	8 32.0%	14 56.0%	2 8.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
5.1.10 Are areas containing confidential information properly secured?	25	2 8.0%	13 52.0%	6 24.0%	4 16.0%	3 12.0%	13 52.0%	9 36.0%	
5.1.11 Are workstations secured after hours?	25	1 4.0%	11 44.0%	10 40.0%	3 12.0%	2 8.0%	11 44.0%	11 44.0%	1 4.0%
5.1.12 Are keys and access cards properly managed?	25	1 4.0%	18 72.0%	5 20.0%	1 4.0%	4 16.0%	18 72.0%	3 12.0%	
5.1.13 Are access cards/ID badges properly displayed?	25	3 12.0%	13 52.0%	7 28.0%	2 8.0%	3 12.0%	16 64.0%	5 20.0%	1 4.0%
5.1.14 Are contract crews activities monitored?	25	1 4.0%	12 48.0%	8 32.0%	4 16.0%	1 4.0%	16 64.0%	6 24.0%	2 8.0%
5.2.1 Have all physical threats been considered?	25	1 4.0%	8 32.0%	7 28.0%	9 36.0%		11 44.0%	9 36.0%	5 20.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
5.2.2 Are power supplies protected from power failures or surges?	25		15 60.0%	8 32.0%	2 8.0%	3 12.0%	16 64.0%	6 24.0%	
5.2.3 Is cabling equipment protected from interception or damage?	25		15 60.0%	6 24.0%	4 16.0%	2 8.0%	13 52.0%	8 32.0%	2 8.0%
5.2.4 Is equipment maintained to vendor specifications?	25	3 12.0%	15 60.0%	3 12.0%	4 16.0%	3 12.0%	16 64.0%	5 20.0%	1 4.0%
5.2.5 Is off-premise equipment inventoried and protected?	23		13 56.5%	8 34.8%	2 8.7%		16 69.6%	7 30.4%	
5.2.6 Is equipment securely disposed?	25	1 4.0%	13 52.0%	6 24.0%	5 20.0%	3 12.0%	12 48.0%	7 28.0%	3 12.0%
5.3.1 Are physical documents adequately protected?	25	3 12.0%	10 40.0%	7 28.0%	5 20.0%	2 8.0%	14 56.0%	9 36.0%	

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
5.3.2 Is there a well-defined process for destruction of critical documents (burn bags, shredding, etc.)?	25	2 8.0%	5 20.0%	11 44.0%	7 28.0%	2 8.0%	10 40.0%	11 44.0%	2 8.0%
5.3.3 Are the visits by maintenance and cleaning staff documented and scheduled?	24	2 8.3%	13 54.2%	6 25.0%	3 12.5%	3 12.5%	14 58.3%	5 20.8%	2 8.3%
6.1.1 Are there complete, approved operating policies and procedures?	25	1 4.0%	6 24.0%	12 48.0%	6 24.0%	1 4.0%	8 32.0%	13 52.0%	3 12.0%
6.1.2 Is there a complete operations change control process?	25	2 8.0%	5 20.0%	6 24.0%	12 48.0%	2 8.0%	9 36.0%	6 24.0%	8 32.0%
6.1.3 Are there documented incident reporting and response procedures?	25	2 8.0%	7 28.0%	7 28.0%	9 36.0%	1 4.0%	7 28.0%	12 48.0%	5 20.0%
6.1.4 Are there complete and defined investigative procedures in place?	25	1 4.0%	5 20.0%	5 20.0%	14 56.0%	1 4.0%	7 28.0%	12 48.0%	5 20.0%

Distribution of Quality and Execution Scores by Question

Question		# Respon	Best Practice	Quality Scores			Execution Scores			
				Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
6.1.5	Are there clearly documented operational roles and responsibilities?	25		10 40.0%	12 48.0%	3 12.0%		13 52.0%	11 44.0%	1 4.0%
6.1.6	Are there documented operational plans for recovery from security incidents?	25		5 20.0%	7 28.0%	13 52.0%		8 32.0%	10 40.0%	7 28.0%
6.1.7	Are duties segregated as appropriate?	25		10 40.0%	10 40.0%	5 20.0%	1 4.0%	15 60.0%	6 24.0%	3 12.0%
6.1.8	Are test development, test and operation facilities clearly delineated and separated?	25	4 16.0%	13 52.0%	4 16.0%	4 16.0%	3 12.0%	14 56.0%	5 20.0%	3 12.0%
6.1.9	Is there effective security coordination between the agency and third-party providers (e.g., OIT, outsourcers, managed services providers, etc.)?	24	1 4.2%	15 62.5%	6 25.0%	2 8.3%	3 12.5%	14 58.3%	5 20.8%	2 8.3%
6.2.1	Is there a process to security certify all new system implementations?	25	2 8.0%	6 24.0%	6 24.0%	11 44.0%	3 12.0%	6 24.0%	10 40.0%	6 24.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
6.2.2 Is there a complete set of multi-level virus control processes and technologies in place (e.g., virus, Trojans, etc.)?	25	7 28.0%	12 48.0%	5 20.0%	1 4.0%	6 24.0%	15 60.0%	4 16.0%	
6.2.3 Are there systematic patch control and upgrade processes in place?	25	3 12.0%	10 40.0%	7 28.0%	5 20.0%	2 8.0%	10 40.0%	13 52.0%	
6.2.4 Are there appropriate recovery plans for virus or malicious software attacks?	25		6 24.0%	11 44.0%	8 32.0%	1 4.0%	12 48.0%	11 44.0%	1 4.0%
6.3.1 Are backup, restore and test processes appropriate to system/data criticality?	25	2 8.0%	14 56.0%	7 28.0%	2 8.0%	2 8.0%	13 52.0%	10 40.0%	
6.3.2 Are consistent operator fault/repair and maintenance logs maintained for all equipment?	25	3 12.0%	10 40.0%	5 20.0%	7 28.0%	3 12.0%	9 36.0%	8 32.0%	5 20.0%
6.3.3 Are telephone usage logs reviewed on a regular basis to discover potential usage abuse?	25	5 20.0%	9 36.0%	5 20.0%	6 24.0%	5 20.0%	9 36.0%	6 24.0%	5 20.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
6.3.4 Are employees made aware of their responsibility to keep remote access codes secure from unauthorized access and/or usage?	25	2 8.0%	14 56.0%	7 28.0%	2 8.0%	1 4.0%	16 64.0%	7 28.0%	1 4.0%
6.3.5 Are portable computer users provided with a mechanism to allow backup of appropriate sensitive information or a critical application to a server or to portable storage media?	24	3 12.5%	9 37.5%	6 25.0%	6 25.0%	3 12.5%	12 50.0%	7 29.2%	2 8.3%
6.4.1 Are there adequate controls for access to the network?	25	4 16.0%	12 48.0%	4 16.0%	5 20.0%	3 12.0%	11 44.0%	8 32.0%	3 12.0%
6.4.2 Are there adequate controls to identify security events?	25	2 8.0%	11 44.0%	5 20.0%	7 28.0%	1 4.0%	9 36.0%	11 44.0%	4 16.0%
6.4.3 Is the network managed with consistent policies and procedures?	25		9 36.0%	10 40.0%	6 24.0%		12 48.0%	9 36.0%	4 16.0%
6.5.1 Are there appropriate procedures for removable computer media (e.g., disk, Zips, flash cards, etc.)?	25		12 48.0%	6 24.0%	7 28.0%		12 48.0%	8 32.0%	5 20.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
6.5.2 Are there consistent processes for the destruction of critical media?	25	2 8.0%	7 28.0%	9 36.0%	7 28.0%	1 4.0%	13 52.0%	9 36.0%	2 8.0%
6.5.3 Is media with the same level of sensitivity (whether electronic or physical) managed with consistent policies and procedures?	25	1 4.0%	8 32.0%	8 32.0%	8 32.0%		12 48.0%	10 40.0%	3 12.0%
6.5.4 Are media-handling procedures appropriate to the data stored?	25		8 32.0%	10 40.0%	7 28.0%		13 52.0%	9 36.0%	3 12.0%
6.6.1 Do verified security agreements and/or documented processes exist with external information exchange partners?	23		12 52.2%	6 26.1%	5 21.7%	1 4.3%	12 52.2%	5 21.7%	5 21.7%
6.6.2 Is encryption (including non-repudiation, identifications, validation, etc.) effectively applied between information exchange partners based on regulatory requirements?	18	1 5.6%	5 27.8%	7 38.9%	5 27.8%	1 5.6%	6 33.3%	7 38.9%	4 22.2%
6.6.3 Are appropriate controls in place to secure e-government/e-commerce projects?	20	2 10.0%	12 60.0%	4 20.0%	2 10.0%	1 5.0%	14 70.0%	3 15.0%	2 10.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
6.6.4 Are incident reports issued to appropriate management?	25	4 16.0%	7 28.0%	9 36.0%	5 20.0%	2 8.0%	11 44.0%	10 40.0%	2 8.0%
6.6.5 After an incident, are policies and procedures reviewed to determine if modifications need to be implemented?	25	2 8.0%	7 28.0%	9 36.0%	7 28.0%	2 8.0%	11 44.0%	8 32.0%	4 16.0%
6.6.6 Are electronic mail protection policies clearly defined, communicated and enforced?	24	2 8.3%	17 70.8%	4 16.7%	1 4.2%	1 4.2%	17 70.8%	5 20.8%	1 4.2%
6.6.7 Are there effective technologies in place to protect electronic mail?	22	2 9.1%	11 50.0%	7 31.8%	2 9.1%	2 9.1%	14 63.6%	6 27.3%	
6.6.8 Are there effective PSPs and technologies in place to secure electronic office systems, e.g., voice, fax, voicemail, wireless and instant messaging?	25	1 4.0%	7 28.0%	6 24.0%	11 44.0%	1 4.0%	10 40.0%	9 36.0%	5 20.0%
6.6.9 Are publicly available systems (e.g., Web servers, FTP sites, etc.) effectively protected?	23	4 17.4%	6 26.1%	8 34.8%	5 21.7%	3 13.0%	8 34.8%	8 34.8%	4 17.4%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.1.1 Are there systematic processes to review individual business applications for security requirements?	25	1 4.0%	6 24.0%	11 44.0%	7 28.0%	1 4.0%	12 48.0%	8 32.0%	4 16.0%
7.1.2 Has the agency performed an assessment on all systems to determine regulatory and contractual requirements effecting system access?	25	1 4.0%	9 36.0%	9 36.0%	6 24.0%	2 8.0%	12 48.0%	6 24.0%	5 20.0%
7.1.3 Access control policies exist and are clearly defined for all applications and systems?	25	1 4.0%	14 56.0%	6 24.0%	4 16.0%	1 4.0%	16 64.0%	7 28.0%	1 4.0%
7.1.4 Is confidential information properly secured?	25		14 56.0%	7 28.0%	4 16.0%	2 8.0%	14 56.0%	8 32.0%	1 4.0%
7.2.1 Are there clearly defined user registration and de-registration processes for each application and system?	25	2 8.0%	13 52.0%	7 28.0%	3 12.0%	2 8.0%	14 56.0%	7 28.0%	2 8.0%
7.2.2 Are access privileges to systems well defined by user role and tracked?	25		13 52.0%	9 36.0%	3 12.0%	1 4.0%	15 60.0%	8 32.0%	1 4.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.2.3 Are there periodic audits of user access to systems and privileges?	25	1 4.0%	8 32.0%	8 32.0%	8 32.0%	2 8.0%	9 36.0%	11 44.0%	3 12.0%
7.2.4 Are there periodic reviews of user access rights and privileges?	25	1 4.0%	8 32.0%	8 32.0%	8 32.0%	1 4.0%	12 48.0%	11 44.0%	1 4.0%
7.2.5 Are there clear policies for assigning, changing and refreshing user passwords based on system/information criticality?	25	1 4.0%	13 52.0%	7 28.0%	4 16.0%	1 4.0%	13 52.0%	10 40.0%	1 4.0%
7.2.6 Are authentication mechanisms appropriate to the degree of access for systems?	25	1 4.0%	15 60.0%	6 24.0%	3 12.0%	1 4.0%	18 72.0%	4 16.0%	2 8.0%
7.2.7 Is there a regular, systematic process to test user passwords for strength and appropriateness?	25		5 20.0%	6 24.0%	14 56.0%		6 24.0%	5 20.0%	14 56.0%
7.2.8 Are passwords and/or accounts being shared?	25	1 4.0%	13 52.0%	8 32.0%	3 12.0%	1 4.0%	10 40.0%	13 52.0%	1 4.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.2.9 Are unsecured user accounts (e.g., guests) still active?	25	4 16.0%	16 64.0%	1 4.0%	4 16.0%	6 24.0%	17 68.0%	2 8.0%	
7.2.10 Are temporary user accounts restricted and disabled in a timely fashion?	24	5 20.8%	11 45.8%	5 20.8%	3 12.5%	7 29.2%	12 50.0%	4 16.7%	1 4.2%
7.2.11 Have employees been trained on proper password management?	25		10 40.0%	11 44.0%	4 16.0%		11 44.0%	11 44.0%	3 12.0%
7.2.12 Are users of all Company-provided network resources required to change the initial default password?	25	5 20.0%	11 44.0%	7 28.0%	2 8.0%	7 28.0%	13 52.0%	4 16.0%	1 4.0%
7.2.13 Are there procedures to password protect (or other relevant technology) unattended end-user equipment?	25	2 8.0%	11 44.0%	6 24.0%	6 24.0%	1 4.0%	10 40.0%	11 44.0%	3 12.0%
7.3.1 Have there been clearly defined and communicated appropriate use policies for remote access?	25	2 8.0%	8 32.0%	7 28.0%	8 32.0%	1 4.0%	12 48.0%	6 24.0%	6 24.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.3.2 Are all unauthorized communication devices deactivated (e.g., modems removed from network attached PCs)?	25	1 4.0%	16 64.0%	4 16.0%	4 16.0%	8 32.0%	14 56.0%	2 8.0%	1 4.0%
7.3.3 Are there appropriate authentication mechanisms for remote access?	24	2 8.3%	10 41.7%	8 33.3%	4 16.7%	2 8.3%	12 50.0%	7 29.2%	3 12.5%
7.3.4 Have remote diagnostics ports been identified and controlled appropriately?	24	3 12.5%	10 41.7%	7 29.2%	4 16.7%	3 12.5%	14 58.3%	4 16.7%	3 12.5%
7.3.5 Is access to other networks actively managed between network administrators?	23	3 13.0%	14 60.9%	2 8.7%	4 17.4%	2 8.7%	17 73.9%	3 13.0%	1 4.3%
7.3.6 Has appropriate technology been deployed to control network access (e.g., Firewalls, VPNs, Radius, etc)?	25	4 16.0%	7 28.0%	7 28.0%	7 28.0%	4 16.0%	9 36.0%	8 32.0%	4 16.0%
7.4.1 Is there a process to track all successful and attempted systems logins?	25	2 8.0%	8 32.0%	10 40.0%	5 20.0%	1 4.0%	7 28.0%	14 56.0%	3 12.0%

Distribution of Quality and Execution Scores by Question

Question		# Respon	Quality Scores				Execution Scores			
			Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.4.2	Have systems been designed to enforce that all systems logins are performed through secure mechanisms (e.g., no clear text passwords)?	25	1 4.0%	8 32.0%	10 40.0%	6 24.0%	2 8.0%	10 40.0%	9 36.0%	4 16.0%
7.4.3	Are system clocks accurately set and protected?	25	4 16.0%	11 44.0%	5 20.0%	5 20.0%	4 16.0%	15 60.0%	5 20.0%	1 4.0%
7.4.4	Are there restrictive policies for providing root-level system access?	25	2 8.0%	12 48.0%	4 16.0%	7 28.0%	3 12.0%	14 56.0%	4 16.0%	4 16.0%
7.4.5	Is root-level system access tracked?	25		11 44.0%	7 28.0%	7 28.0%		11 44.0%	9 36.0%	5 20.0%
7.4.6	Has a password management system been designed that is appropriate to the agencies environment (e.g., turnover rate, use of contractors, public access)?	25		12 48.0%	9 36.0%	4 16.0%		14 56.0%	9 36.0%	2 8.0%
7.4.7	Are the desktop platforms secured?	25	1 4.0%	9 36.0%	10 40.0%	5 20.0%	2 8.0%	5 20.0%	16 64.0%	2 8.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.4.8 Are the host systems and servers, as well as application servers, secured?	25	1 4.0%	13 52.0%	6 24.0%	5 20.0%	2 8.0%	14 56.0%	6 24.0%	3 12.0%
7.4.9 Are audit tools protected from unauthorized access?	21	2 9.5%	9 42.9%	5 23.8%	5 23.8%	3 14.3%	11 52.4%	4 19.0%	3 14.3%
7.4.10 Are inactive sessions and terminals terminated from system access?	25	1 4.0%	10 40.0%	9 36.0%	5 20.0%	1 4.0%	13 52.0%	9 36.0%	2 8.0%
7.5.1 Is user access restricted to required systems?	25	1 4.0%	16 64.0%	5 20.0%	3 12.0%	3 12.0%	17 68.0%	4 16.0%	1 4.0%
7.5.2 Are there controls in place to ensure that applications can not corrupt the operating system or security environments?	25	1 4.0%	12 48.0%	8 32.0%	4 16.0%	2 8.0%	16 64.0%	3 12.0%	4 16.0%
7.5.3 Are controls in place at the application level to protect sensitive data?	24		14 58.3%	7 29.2%	3 12.5%		17 70.8%	5 20.8%	2 8.3%

Distribution of Quality and Execution Scores by Question

Question		Quality Scores					Execution Scores			
		# Respon	Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.5.4	Has sensitive information been identified and linked to specific applications?	24	1	10	9	4	1	14	8	1
			4.2%	41.7%	37.5%	16.7%	4.2%	58.3%	33.3%	4.2%
7.5.5	Is use of applications being monitored on a user basis?	25		7	9	9	1	6	12	6
				28.0%	36.0%	36.0%	4.0%	24.0%	48.0%	24.0%
7.5.6	Are applications logs reviewed on a scheduled basis for security events?	25	1	7	9	8	2	8	10	5
			4.0%	28.0%	36.0%	32.0%	8.0%	32.0%	40.0%	20.0%
7.5.7	Is there process in place to ensure that logging is in place and that log files can not be deleted?	25		8	7	10		12	5	8
				32.0%	28.0%	40.0%		48.0%	20.0%	32.0%
7.6.1	Are mobile devices secured (e.g., passwords, time-outs, etc.)?	25	1	11	5	8	3	6	12	4
			4.0%	44.0%	20.0%	32.0%	12.0%	24.0%	48.0%	16.0%
7.6.2	Do mobile devices have secure communications channels (e.g., sFTP, VPN, PGP, etc.)?	22	2	7	8	5	1	9	9	3
			9.1%	31.8%	36.4%	22.7%	4.5%	40.9%	40.9%	13.6%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.6.3 Do mobile devices have tested, secure configurations?	25	1 4.0%	7 28.0%	9 36.0%	8 32.0%	1 4.0%	8 32.0%	10 40.0%	6 24.0%
7.6.4 Are there policies defining types of data allowed on specific mobile appliances?	25	1 4.0%	6 24.0%	5 20.0%	13 52.0%	1 4.0%	4 16.0%	10 40.0%	10 40.0%
7.6.5 Is there a telecommuting PSP?	23	1 4.3%	8 34.8%	7 30.4%	7 30.4%	1 4.3%	9 39.1%	8 34.8%	5 21.7%
7.6.6 Are there policies defining the encryption/security requirements for different mobile devices?	25		6 24.0%	9 36.0%	10 40.0%		5 20.0%	13 52.0%	7 28.0%
7.7.1 Is the network environment partitioned according to security requirements?	25	6 24.0%	4 16.0%	7 28.0%	8 32.0%	6 24.0%	4 16.0%	8 32.0%	7 28.0%
7.7.2 Do network and system administrators have adequate experience to implement security standards?	25	2 8.0%	10 40.0%	9 36.0%	4 16.0%	1 4.0%	13 52.0%	10 40.0%	1 4.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.7.3 Are report logs reviewed and reconciled on a regular basis?	25	1 4.0%	4 16.0%	11 44.0%	9 36.0%	1 4.0%	6 24.0%	13 52.0%	5 20.0%
7.7.4 Are administrators using appropriate tools to perform their jobs?	25		8 32.0%	12 48.0%	5 20.0%		12 48.0%	12 48.0%	1 4.0%
7.7.5 Is there a current network diagram available?	25	5 20.0%	12 48.0%	5 20.0%	3 12.0%	6 24.0%	12 48.0%	5 20.0%	2 8.0%
7.7.6 Are access control lists (ACL) maintained on a regular basis?	22	2 9.1%	6 27.3%	8 36.4%	6 27.3%	3 13.6%	10 45.5%	8 36.4%	1 4.5%
7.7.7 Is there a remote access procedure in place?	25	1 4.0%	10 40.0%	8 32.0%	6 24.0%	2 8.0%	13 52.0%	5 20.0%	5 20.0%
7.7.8 Are critical servers protected with appropriate access control?	25	2 8.0%	13 52.0%	6 24.0%	4 16.0%	1 4.0%	13 52.0%	9 36.0%	2 8.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.7.9 Is the network infrastructure audited on a regular basis?	25	1 4.0%	2 8.0%	11 44.0%	11 44.0%	1 4.0%	2 8.0%	12 48.0%	10 40.0%
7.7.10 Are network vulnerability assessments conducted?	25	1 4.0%	4 16.0%	8 32.0%	12 48.0%	1 4.0%	3 12.0%	11 44.0%	10 40.0%
7.7.11 Is there a policy to prohibit the use of audit tools (e.g., sniffers) by non-authorized individuals?	25	3 12.0%	4 16.0%	7 28.0%	11 44.0%	2 8.0%	8 32.0%	5 20.0%	10 40.0%
7.7.12 Has a demilitarized zone (DMZ) or perimeter network (a segment of network between the router that connects to the Internet and the firewall) been implemented?	25	6 24.0%	6 24.0%	5 20.0%	8 32.0%	6 24.0%	8 32.0%	6 24.0%	5 20.0%
7.7.13 Are changes/improvements made in a timely fashion following network vulnerability assessments?	23	1 4.3%	7 30.4%	7 30.4%	8 34.8%	1 4.3%	10 43.5%	7 30.4%	5 21.7%
7.8.1 Are only approved protocols allowed to go across firewalls?	25	3 12.0%	9 36.0%	7 28.0%	6 24.0%	4 16.0%	11 44.0%	6 24.0%	4 16.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.8.2 Has a risk analysis been conducted to determine if the protocols allowed maintain an acceptable level of risk?	25	1 4.0%	6 24.0%	7 28.0%	11 44.0%		9 36.0%	7 28.0%	9 36.0%
7.8.3 Has the firewall been tested to determine if outside penetration is possible?	25	1 4.0%	7 28.0%	5 20.0%	12 48.0%	1 4.0%	6 24.0%	9 36.0%	9 36.0%
7.8.4 Are other products in place to augment the firewall level of security?	25	3 12.0%	9 36.0%	6 24.0%	7 28.0%	4 16.0%	9 36.0%	6 24.0%	6 24.0%
7.8.5 Are firewalls maintained and monitored around the clock?	25	2 8.0%	10 40.0%	6 24.0%	7 28.0%	4 16.0%	8 32.0%	8 32.0%	5 20.0%
7.9.1 Do you have a wireless policy?	25	2 8.0%	10 40.0%	4 16.0%	9 36.0%	2 8.0%	10 40.0%	8 32.0%	5 20.0%
7.9.2 Is the wireless policy in compliance with the State Security PSP?	23	4 17.4%	9 39.1%	2 8.7%	8 34.8%	4 17.4%	9 39.1%	6 26.1%	4 17.4%

Distribution of Quality and Execution Scores by Question

Question		# Respon	Quality Scores				Execution Scores			
			Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
7.9.3	Are there tests to ensure that approved wireless networks are secure and that there are no unapproved wireless networks?	24	1 4.2%	4 16.7%	2 8.3%	17 70.8%	1 4.2%	3 12.5%	6 25.0%	14 58.3%
7.9.4	Do the wireless networks have a secure configuration, including the use of encrypted transmission and authentication of users?	13	2 15.4%	4 30.8%	2 15.4%	5 38.5%	2 15.4%	4 30.8%	6 46.2%	1 7.7%
8.1.1	Are security requirements determined for all applications?	25	1 4.0%	9 36.0%	11 44.0%	4 16.0%	2 8.0%	15 60.0%	6 24.0%	2 8.0%
8.1.2	Are controls appropriate for the level of risk and value of information?	25	2 8.0%	10 40.0%	8 32.0%	5 20.0%	3 12.0%	16 64.0%	3 12.0%	3 12.0%
8.1.3	Are controls built into all applications?	25		14 56.0%	7 28.0%	4 16.0%	1 4.0%	17 68.0%	5 20.0%	2 8.0%
8.1.4	Are controls regularly monitored and managed?	25		10 40.0%	11 44.0%	4 16.0%	1 4.0%	13 52.0%	9 36.0%	2 8.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
8.1.5 Is security part of all systems implementations and development projects?	25	2 8.0%	11 44.0%	7 28.0%	5 20.0%	3 12.0%	13 52.0%	6 24.0%	3 12.0%
8.2.1 Have areas of system risk been identified?	25	1 4.0%	10 40.0%	9 36.0%	5 20.0%	1 4.0%	14 56.0%	8 32.0%	2 8.0%
8.2.2 Have checks and controls been applied, as appropriate (e.g., balancing, hash totals)?	24	1 4.2%	10 41.7%	8 33.3%	5 20.8%	1 4.2%	16 66.7%	4 16.7%	3 12.5%
8.2.3 Is SSL (or other appropriate secure communications) used for secure internet system-to-system communication?	24	5 20.8%	13 54.2%	2 8.3%	4 16.7%	6 25.0%	11 45.8%	2 8.3%	5 20.8%
8.3.1 Are end-user and application-manager-specific policies and procedures about the relevant use of encryption used appropriately?	24		8 33.3%	8 33.3%	8 33.3%		13 54.2%	4 16.7%	7 29.2%
8.3.2 Are digital signatures for non-repudiation used appropriately?	15		5 33.3%	5 33.3%	5 33.3%	1 6.7%	5 33.3%	5 33.3%	4 26.7%

Distribution of Quality and Execution Scores by Question

Question	Quality Scores					Execution Scores			
	# Respon	Best Practice	Meets Reqmn't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
8.3.3 Are cryptographic keys protected, where applicable?	10	1 10.0%	3 30.0%	4 40.0%	2 20.0%	1 10.0%	5 50.0%	3 30.0%	1 10.0%
8.3.4 Is there a certified key management system?	8	1 12.5%	2 25.0%	1 12.5%	4 50.0%	1 12.5%	2 25.0%	1 12.5%	4 50.0%
8.4.1 Is purchased software (new and upgrades) security assured in a test environment before promotion or implementation?	24		9 37.5%	9 37.5%	6 25.0%		12 50.0%	7 29.2%	5 20.8%
8.4.2 Is there a controlled process for updating system/application libraries?	25	2 8.0%	12 48.0%	8 32.0%	3 12.0%	1 4.0%	15 60.0%	6 24.0%	3 12.0%
8.4.3 Is system test data given the same level of security protection as production data?	25	1 4.0%	12 48.0%	7 28.0%	5 20.0%	4 16.0%	12 48.0%	6 24.0%	3 12.0%
8.4.4 Is there control and logging of access to the system source libraries?	25	3 12.0%	11 44.0%	8 32.0%	3 12.0%	4 16.0%	13 52.0%	5 20.0%	3 12.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
8.5.1 Are there formal change control procedures?	25	2 8.0%	8 32.0%	7 28.0%	8 32.0%	1 4.0%	11 44.0%	8 32.0%	5 20.0%
8.5.2 Are there security and technology reviews of system changes before promotion to production?	25	2 8.0%	9 36.0%	10 40.0%	4 16.0%	1 4.0%	14 56.0%	8 32.0%	2 8.0%
8.5.3 Is there a documentation process that effectively captures system and applications changes and upgrades?	25	2 8.0%	11 44.0%	7 28.0%	5 20.0%	2 8.0%	16 64.0%	4 16.0%	3 12.0%
8.5.4 Are back door and covert channels into applications identified and closed?	25	3 12.0%	6 24.0%	10 40.0%	6 24.0%	3 12.0%	10 40.0%	7 28.0%	5 20.0%
8.5.5 Does outsourced software development subscribe to the Agency's security policies and procedures?	17		11 64.7%	2 11.8%	4 23.5%	2 11.8%	8 47.1%	5 29.4%	2 11.8%
8.6.1 Has an application development methodology been implemented?	25	5 20.0%	10 40.0%	4 16.0%	6 24.0%	4 16.0%	14 56.0%	4 16.0%	3 12.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
8.6.2 Is pre-production testing performed in an isolated environment?	25	2 8.0%	16 64.0%	4 16.0%	3 12.0%	3 12.0%	14 56.0%	5 20.0%	3 12.0%
9.1.1 Has a business impact analysis (BIA)/risk assessment been conducted?	25		8 32.0%	4 16.0%	13 52.0%	1 4.0%	6 24.0%	9 36.0%	9 36.0%
9.1.2 Has continuity planning that includes identification of RTO and RPO for time-critical data, programs, documentation been identified?	25	2 8.0%	6 24.0%	7 28.0%	10 40.0%	2 8.0%	7 28.0%	7 28.0%	9 36.0%
9.1.3 Is the BIA reviewed and updated regularly?	22		7 31.8%	3 13.6%	12 54.5%	1 4.5%	5 22.7%	7 31.8%	9 40.9%
9.1.4 Does executive management review and approve the prioritized list of time-critical recovery requirements?	22		10 45.5%	5 22.7%	7 31.8%	1 4.5%	9 40.9%	6 27.3%	6 27.3%
9.2.1 Has a crisis management or BCP coordinator been named?	25	6 24.0%	7 28.0%	8 32.0%	4 16.0%	3 12.0%	9 36.0%	10 40.0%	3 12.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
9.2.2 Are system, application and data backups sent to a secure off-site facility on a regular basis?	25	2 8.0%	14 56.0%	5 20.0%	4 16.0%	2 8.0%	13 52.0%	7 28.0%	3 12.0%
9.2.3 Are there copies of the DR plans? (collect two copies on CD from the agencies)	25	6 24.0%	12 48.0%	3 12.0%	4 16.0%	7 28.0%	11 44.0%	3 12.0%	4 16.0%
9.2.4 Have continuity and disaster scenarios been developed?	24	3 12.5%	6 25.0%	10 41.7%	5 20.8%	3 12.5%	5 20.8%	11 45.8%	5 20.8%
9.2.5 Are remote recovery facilities located in geographical location unlikely to be affected by the same disruption?	25	2 8.0%	12 48.0%	4 16.0%	7 28.0%	2 8.0%	12 48.0%	4 16.0%	7 28.0%
9.2.6 Do contracts for outsourced activities include service providers' responsibilities for continuity planning?	23	2 8.7%	11 47.8%	3 13.0%	7 30.4%	2 8.7%	9 39.1%	5 21.7%	7 30.4%
9.2.7 Are critical inventories (i.e., hardware, software, communications equipment, facilities, people, working space, documentation data transportation, etc.) in place?	25	3 12.0%	9 36.0%	5 20.0%	8 32.0%	3 12.0%	6 24.0%	11 44.0%	5 20.0%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
9.2.8 Is a copy of the continuity plan stored at the backup site, and is it updated regularly?	22	3 13.6%	9 40.9%	4 18.2%	6 27.3%	3 13.6%	7 31.8%	7 31.8%	5 22.7%
9.2.9 Are contingency arrangements in place for hardware, software, communications facilities, business operations and supporting staffing?	24	1 4.2%	6 25.0%	7 29.2%	10 41.7%	1 4.2%	7 29.2%	10 41.7%	6 25.0%
9.2.10 Are the DR and off-site storage facility locations assessed for security?	22		9 40.9%	6 27.3%	7 31.8%	1 4.5%	10 45.5%	5 22.7%	6 27.3%
9.3.1 Are there training sessions for all relevant personnel in the areas of backup, recovery, crisis management and contingency operating procedures?	25		5 20.0%	10 40.0%	10 40.0%		4 16.0%	15 60.0%	6 24.0%
9.3.2 Has the DR plan been tested?	22	2 9.1%	5 22.7%	9 40.9%	6 27.3%	4 18.2%	3 13.6%	11 50.0%	4 18.2%
9.3.3 Is there an active process for reviewing and evergreening the BCP plan?	23	2 8.7%	9 39.1%	6 26.1%	6 26.1%	3 13.0%	8 34.8%	8 34.8%	4 17.4%

Distribution of Quality and Execution Scores by Question

Question	# Respon	Quality Scores				Execution Scores			
		Best Practice	Meets Reqmn't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
9.4.1 Are there provisions in place to maintain the security of business operations and IT processing functions in the event of an emergency?	25	2 8.0%	9 36.0%	4 16.0%	10 40.0%	1 4.0%	9 36.0%	7 28.0%	8 32.0%
10.1.1 Is there a documented list of all applicable legislation and specific controls required?	25	2 8.0%	11 44.0%	6 24.0%	6 24.0%	2 8.0%	12 48.0%	7 28.0%	4 16.0%
10.1.2 Are there policies to protect intellectual property rights (e.g., piracy, licensing, source code) of purchased software?	25	6 24.0%	7 28.0%	8 32.0%	4 16.0%	3 12.0%	11 44.0%	9 36.0%	2 8.0%
10.1.3 Has a records retention policy been identified?	25	1 4.0%	16 64.0%	6 24.0%	2 8.0%		13 52.0%	11 44.0%	1 4.0%
10.1.4 Is there an audit process to assure adherence to the records retention policy?	25	2 8.0%	8 32.0%	2 8.0%	13 52.0%	1 4.0%	8 32.0%	6 24.0%	10 40.0%
10.1.5 Are there appropriate protections for privacy and confidentiality (e.g., HIPAA, FERPA, etc.) as required by legislation?	20	1 5.0%	11 55.0%	5 25.0%	3 15.0%	1 5.0%	15 75.0%	3 15.0%	1 5.0%

Distribution of Quality and Execution Scores by Question

Question		# Respon	Quality Scores				Execution Scores			
			Best Practice	Meets Reqm't	Deficient	Does Not meet Reqmn't	Fully Meets	Critical Areas	Minimal / Gaps	None / WIP
10.1.6	Are there access warning messages to indicate appropriate use of data/system access?	25	4 16.0%	13 52.0%	1 4.0%	7 28.0%	5 20.0%	11 44.0%	2 8.0%	7 28.0%
10.2.1	Has a compliance review of security policies been performed in the past year?	24	2 8.3%	3 12.5%	3 12.5%	16 66.7%	3 12.5%	3 12.5%	6 25.0%	12 50.0%
10.2.2	Has a technical compliance check been performed (i.e., vulnerability test) in the past year?	25	1 4.0%	4 16.0%	7 28.0%	13 52.0%	1 4.0%	4 16.0%	10 40.0%	10 40.0%

***** End of Report *****